FY 1999

NATIONAL COMMUNICATIONS SYSTEM

Leading Technology Excellence into the New Millennium

Meeting the challenges of the Year 2000 and beyond will require world-class leadership and superior technology solutions. For over 35 years, the National Communications System (NCS) has ensured that the Federal Government possesses the telecommunications resources necessary to meet the United States' national security and emergency preparedness responsibilities under all circumstances. Building on the successful history of interagency cooperation and industry/Government partnership, the NCS will help lead the Nation into the 21st century.

NATIONAL COMMUNICATIONS SYSTEM

PREPARED BY THE OFFICE OF THE MANAGER, NATIONAL COMMUNICATIONS SYSTEM

Leading Technology Excellence into the New Millennium

2

FOREWORD

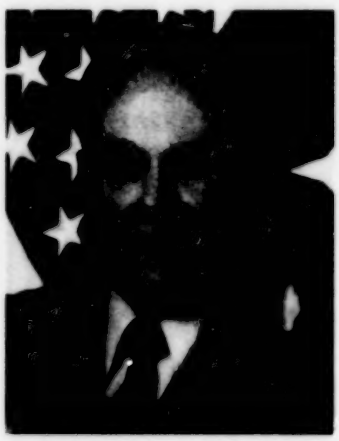
As Manager of the National Communications System (NCS), I am proud to lead the efforts to meet the telecommunications needs of the Nation's national security and emergency preparedness (NS/EP) community, particularly as we prepare for the challenges of the Year 2000 (Y2K) and the new cyber age. Interagency cooperation among the 23 NCS member organizations and the industry/Government partnerships exhibited in the National Coordinating Center for Telecommunications (NCC) and the President's National Security Telecommunications Advisory Committee (NSTAC) continue to be essential to the success of the NCS.

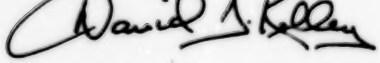
During fiscal year (FY) 1999, the NCS prepared for potential Y2K-induced disruptions to the telecommunications infrastructure by leveraging its working relationships with industry and Government. Working through the NCC, in conjunction with the Office of Science and Technology Policy, the Joint Telecommunications Resources Board, the Y2K Readiness Task Force, industry groups, and international organizations, the NCS helped develop contingency plans and tools essential to the Nation's Y2K readiness and response.

Concurrent with its preparations for Y2K, and in concert with the Administration's commitment to critical infrastructure protection, the NCC worked to enhance its NS/EP telecommunications coordination and response capability. During FY 1999, the NCC began its indications, assessment, and warning operations, which are based on voluntary reporting of electronic intrusion incidents by industry and Government. This has led to the NCC being designated as an Information Sharing and Analysis Center for telecommunications under the provisions of Presidential Decision Directive 63 "Critical Infrastructure Protection."

During FY 1999, the NCS continued to provide NS/EP users with a nationwide capability for emergency access and specialized processing of switched-voice and voice-band data communications through programs such as the Government Emergency Telecommunications Service (GETS). Based on an NSTAC recommendation to the President in June 1999, the NCS has taken preliminary steps to initiate a program to address NS/EP issues related to the Internet, including examination of priority services for packet networks and the implications for existing priority services (such as GETS) resulting from Public Switched Network and Internet convergence.

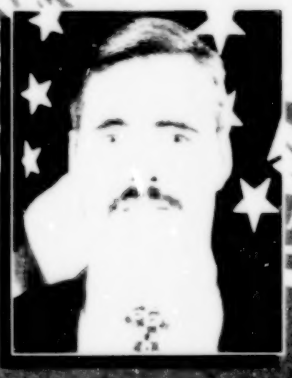
After three and one-half decades, the NCS continues to be a focal point for industry and Government cooperation to ensure that reliable, interoperable, and secure telecommunications are available to fulfill the Nation's NS/EP requirements under all conditions. The existing industry/Government partnership provides a solid foundation upon which we can build to ensure that our future communications needs will be met.





DAVID J. KELLEY
Lieutenant General, USA
Manager

NATIONAL COMMUNICATIONS SYSTEM



Ms. Penn A. Fenton
Chief
Technology and
Programs

Col. Kenny E. Schnoor
USAF
Chief
Operations Division

Mr. Larry E. Wheaton
Chief
Plans and Resources

Mr. Francesco W. Sisto
Chief
Customer Service

NCS COMMITTEE OF PRINCIPALS

Department of State (DOS)
MR. FERNANDO BURBANO

Department of the Treasury (TREAS)
MR. THOMAS C. WEISNER

Department of Defense (DOD)
RADM. ROBERT M. NUTWELL, USN

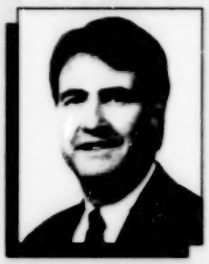
Department of Justice (DOJ)
MR. RICHARD CHAPMAN

Department of the Interior (DOI)
MR. DARYL W. WHITE

United States Department of Agriculture (USDA)
MR. IRA L. HOBBS

Department of Commerce (DOC)
MR. JOROME T. GIBBON

Department of Health and Human Services (DHHS)
DR. ROBERT F. KNOUSS



Department of Transportation (DOT)
MR. EUGENE K. TAYLOR, JR.

Department of Energy (DOE)
MR. JOHN M. GILLIGAN

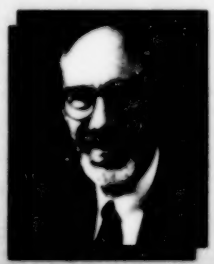
Department of Veterans Affairs (VA)
MR. ROBERT P. BUBNIAK

Federal Emergency Management Agency (FEMA)
MR. G. CLAY HOLLISTER

United States Information Agency (USIA)
MS. MARGARET A. JOHNSON

The Joint Staff (JS)
LTG JOHN L. WOODWARD, JR., USAF

General Services Administration (GSA)
MR. DENNIS J. FISCHER



National Aeronautics and Space Administration (NASA)
MR. ROBERT E. SPEARING

Nuclear Regulatory Commission (NRC)
MR. FRANK J. CONGEL

National Telecommunications and Information Administration (NTIA)
MR. WILLIAM T. HATCH

National Security Agency (NSA)
MR. MICHAEL G. FLEMING

United States Postal Service (USPS)
MR. TIMOTHY J. PATTERSON

Federal Reserve Board (FRB)
MR. KENNETH D. BUCKLEY

Federal Communications Commission (FCC)
MR. ALLAN K. VAN DOORN

NCS COUNCIL OF REPRESENTATIVES

Department of State (DOS)
Ms. Kimberly A. Godwin

Department of the Treasury (TREAS)
Ms. [illegible]

Department of Defense (DOD)
Capt. Todd D. Tracy

Department of Justice (DOJ)
Mr. [illegible]

Department of the Interior (DOI)
Mr. James E. Dolezal

United States Department of Agriculture (USDA)
Ms. Brenda F. Boger

Department of Commerce (DOC)
Ms. Joanne T. Gibson

Department of Health and Human Services (DHHS)
Capt. Michael B. Anderson, USPHS

Department of Transportation (DOT)
Lcdr. Richard W. Wiegand, USCG

Department of Energy (DOE)
Mr. Patrick Hargett

Department of Veterans Affairs (VA)
Mr. Howard D. Boyd

Federal Emergency Management Agency (FEMA)
Dr. Joseph H. Maiba

United States Information Agency (USIA)
Ms. Margaret A. Johnson

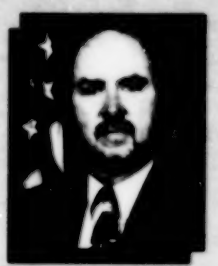
The Joint Staff (JS)
Col. James Arle, USAF

General Services Administration (GSA)
Mr. Thomas E. Sellers

National Aeronautics and Space Administration (NASA)
Ms. [illegible]

Nuclear Regulatory Commission (NRC)
Mr. Joseph G. Gitter

National Telecommunications and Information Administration (NTIA)
Mr. [illegible]



National Security Agency (NSA)
Mr. R. Michael Green

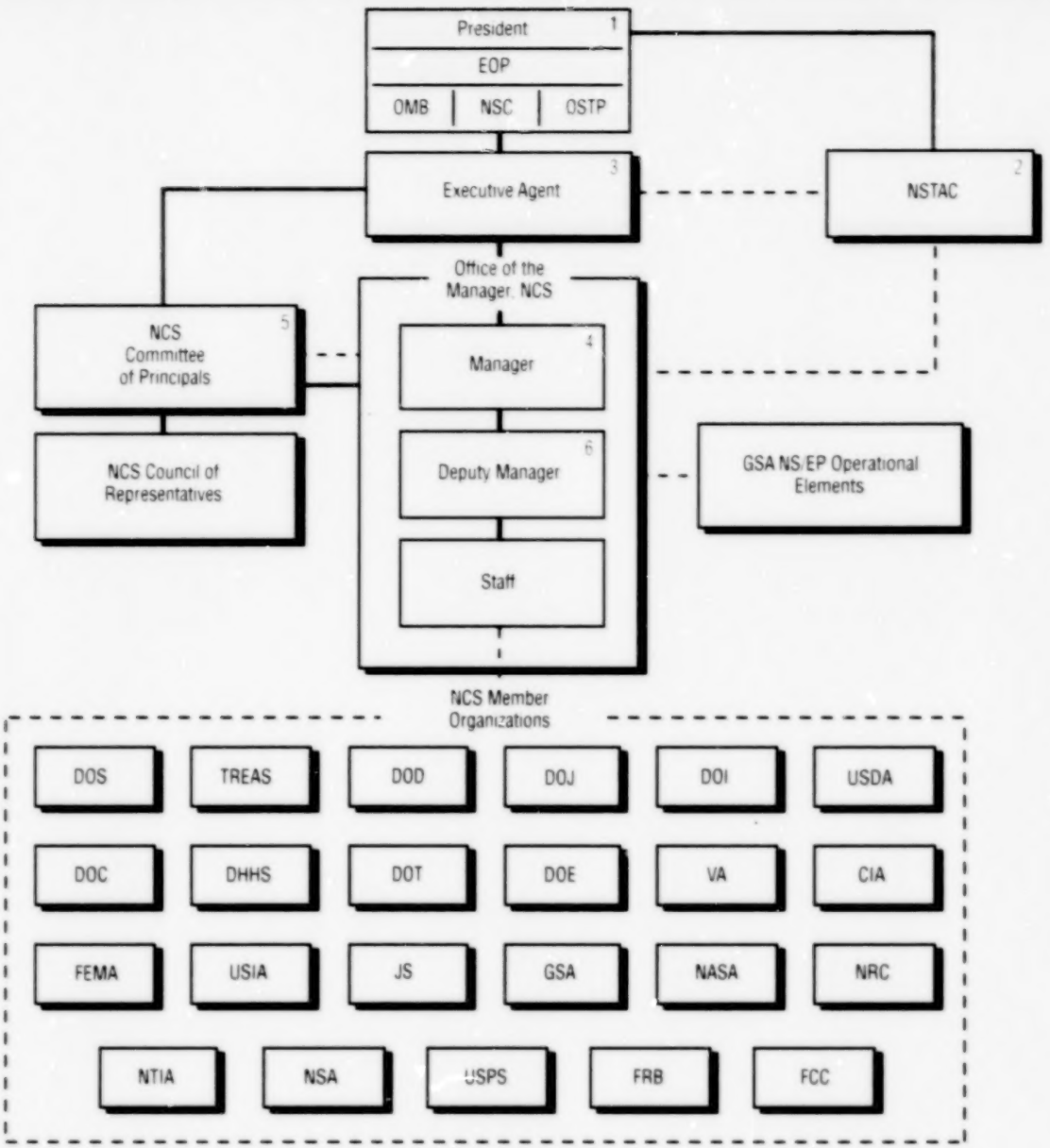
United States Postal Service (USPS)
Ms. [illegible]

Federal Reserve Board (FR3)
Ms. Anne E. Paulin

[illegible]
[illegible]

6

THE NCS ORGANIZATION



1. Policy Direction and Direct Execution of War Powers Functions
2. National Security Telecommunications Advisory Committee
3. Executive Agent, NCS responsibilities assigned to Secretary of Defense by E.O. 12472, April 3, 1984
4. Director, DISA, serves as Manager, NCS
5. The Key Telecommunications Officers of the NCS Member Organizations
6. First line management position that is exclusively NCS

LEGEND
Direction
Coordination
Advice

TABLE OF CONTENTS

	Page Number
I. INTRODUCTION	
Background	1-2
Environment Facing the NCS	1-3
Facing Issues of the 21st Century	1-8
Report Organization	1-8
II. EMERGENCY RESPONSE ACTIVITIES	
NCC 9/9/99 Y2K Emergency Operations Team Activation	2-2
Telecommunications Emergency Response Training	2-3
NCS Regional Managers Conference	2-3
NCS Continuity of Operations Orientation	2-4
III. NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS	
OMNCS Reorganization	3-1
OMNCS Y2K Preparedness Activities	3-1
Technology and Programs	3-7
Operations	3-14
Plans and Resources	3-22
Customer Service	3-23
IV. NS/EP TELECOMMUNICATIONS SUPPORT AND ACTIVITIES OF NCS MEMBER ORGANIZATIONS	
Department of State (DOS)	4-2
Department of the Treasury (TREAS)	4-3
Department of Defense (DOD)	4-4
Department of Justice (DOJ)	4-5
Department of the Interior (DOI)	4-6
United States Department of Agriculture (USDA)	4-7
Department of Commerce (DOC)	4-8
Department of Health and Human Services (DHHS)	4-10
Department of Transportation (DOT)	4-11
Department of Energy (DOE)	4-12
Department of Veterans Affairs (VA)	4-13
Central Intelligence Agency (CIA)	4-14
Federal Emergency Management Agency (FEMA)	4-15
United States Information Agency (USIA)	4-16
The Joint Staff (JS)	4-17
General Services Administration (GSA)	4-18
National Aeronautics and Space Administration (NASA)	4-19
Nuclear Regulatory Commission (NRC)	4-20
National Telecommunications and Information Administration (NTIA)	4-21
National Security Agency (NSA)	4-22
United States Postal Service (USPS)	4-23
Federal Reserve Board (FRB)	4-24
Federal Communications Commission (FCC)	4-25
A. NCS Related Acronyms	

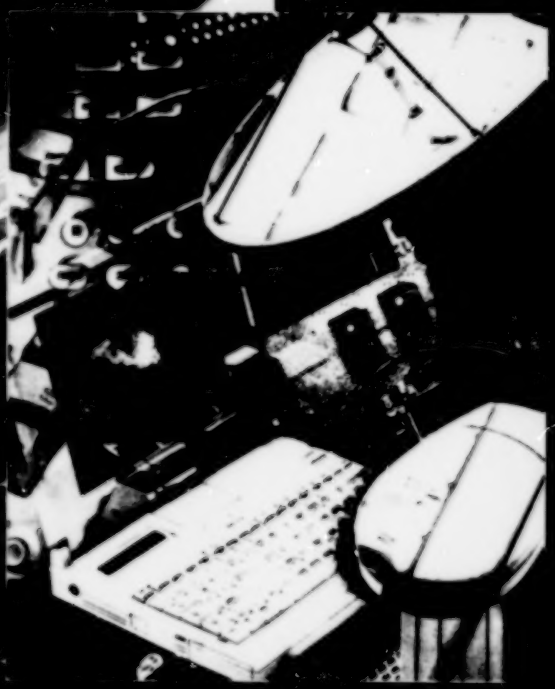
8

LIST OF EXHIBITS

		Page Number
3-1	GETS Operational Concept	3-7
3-2	Technical Notes and Information Bulletins	3-15
3-3	Federal Telecommunications Recommendations	3-15
3-4	Enhanced NTCN Components	3-16
3-5	ERLink Network Architecture	3-22
3-6	The President's National Security Telecommunications Advisory Committee Organization	3-24
3-7	Requirements Identification Benefits	3-30
4-1	Command Control, Communications, and Computer Systems Directorate	4-17

I

INTRODUCTION



INTRODUCTION

The Office of the Manager, National Communications System (OMNCS), in coordination with the National Communications System (NCS) Committee of Principals (COP), publishes the *FY99 National Communications System Report*. This report highlights significant national security and emergency preparedness (NS/EP) telecommunications events and major NCS initiatives, activities, and accomplishments during fiscal year 1999 (FY 1999).

BACKGROUND

The NCS was formed in the wake of communications shortfalls in support of national security decision making during the 1962 Cuban Missile Crisis. Since then the challenges the NCS has faced have evolved with changes in technology, the marketplace, and national security threats.

On August 21, 1963, President Kennedy signed a Presidential Memorandum establishing the NCS and defining its mission. According to this memorandum, the objective of the NCS is to "provide the necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crises, including nuclear attack."

Over the years, the role of telecommunications in supporting the Nation's NS/EP functions expanded, and enhanced emergency telecommunications capabilities became essential. By the late 1970s, Government policy formally recognized that the Nation's telecommunications infrastructure was an essential component of deterrence and recovery in the face of a Soviet nuclear attack. The expanded role of telecommunications was also evident in light of the growing complexity of Government, the rapid growth in telecommunications technologies and services, and the important part telecommunications plays in responding to manmade and natural disasters.

At the same time, the impending divestiture of AT&T and the proliferation of service providers in the industry complicated the means for satisfying NS/EP telecommunications requirements. In anticipation of the loss of a single point of contact within the industry for NS/EP telecommunications planning and service provisioning, President Reagan established the National Security Telecommunications Advisory Committee (NSTAC) by Executive Order 12382 in 1982.

Composed of chief executives from major telecommunications and information technology-related companies, the NSTAC would provide the President with a unified source of national security telecommunications policy expertise unobtainable solely within the Federal Government.

On April 3, 1984, President Reagan signed Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, which revitalized and expanded the NCS. This executive order formally reestablished the NCS structure to include the Secretary of Defense as the Executive Agent; the Manager, NCS, and a staff; and a Committee of Principals, which represents the 23 Federal member organizations. The NCS's basic mission is to assist the Executive Office of the President in the exercise of wartime and nonwartime emergency telecommunications responsibilities, and to coordinate the planning and provisioning of NS/EP communications for the Federal Government under all circumstances.

An important dimension of the rechartered NCS was its mandate to serve as a focal point for industry/Government NS/EP telecommunications planning. While the NCS Committee of Principals served as the mechanism for Federal interagency coordination, the NSTAC and its working group structure became the means for the NCS to work with industry to address the range of NS/EP telecommunications issues.

Through the collective resources of its members and in partnership with industry, the NCS continues to meet the full range of NS/EP telecommunications challenges, from supporting military operations to responding to natural disasters to protecting the telecommunications infrastructure from electronic intrusion. As it has for more than 35 years, the NCS will continue to respond to emerging challenges by leveraging its experience, working relationships, and capabilities to improve the security, reliability, and interoperability of the national telecommunications infrastructure.

ENVIRONMENT FACING THE NCS

EMERGING TELECOMMUNICATIONS MARKETPLACE

The rapid restructuring of the telecommunications marketplace continued in FY 1999, 3 years after passage of the *Telecommunications Act of 1996 (1996 Act)*. The primary focus of the *1996 Act* was to promote competition in both the local exchange market and across market segments. To that end, the 1996 Act mandated regulatory changes to aid the entry of competitive local exchange carriers (CLEC) into the local market. The 1996 Act also eased restrictions on both mergers and ownership limits. In FY 1999, incumbent telecommunications providers continued to seek merger opportunities. At the same time, the Federal Communications Commission (FCC) reported a steady increase in the overall market share held by CLECs. The FCC, meanwhile, continued to promulgate rules guiding the implementation of the *1996 Act*.

The FCC and the Supreme Court issued numerous high-impact decisions in FY 1999. In particular, in January the Supreme Court upheld the vast majority of the FCC's local competition rules, allowing CLECs to more easily compete against incumbents in the local exchange market. Shortly thereafter, the FCC strengthened several of its rules, further aiding new entrants. The incumbent Regional Bell Operating Companies (RBOC) have thus far been unable to meet the conditions required by the FCC to enter the long distance market within their respective regions. Industry observers expect one RBOC's entry by the year 2000, however.

On the merger front, telecommunications carriers continued to merge and partner. Although the Bell Atlantic–GTE, U S WEST-QWEST, and SBC Communications-Ameritech mergers remain pending, observers expect the FCC to approve all three mergers (albeit with conditions) in the near future. Meanwhile, AT&T

completed its purchase of cable company Telecommunications Incorporated (TCI) and has its purchase of cable company MediaOne pending at the FCC and Department of Justice. These telecommunications providers assert this consolidation is necessary to compete in their own market, and across market segments.

On the technology front, "convergence", the ability to offer a variety of services over the same network, is a major issue, with digitalization and packet switching expanding the service offerings and capabilities of all carriers. This trend continues to blur the traditional distinctions between cable, Internet, and telephone industries, as companies form relationships and sell in the other markets. Carriers continued researching and implementing network advances to improve efficiency and enhance competitiveness. Incumbent carriers, in particular, continued to leverage new technology to enhance their legacy networks.

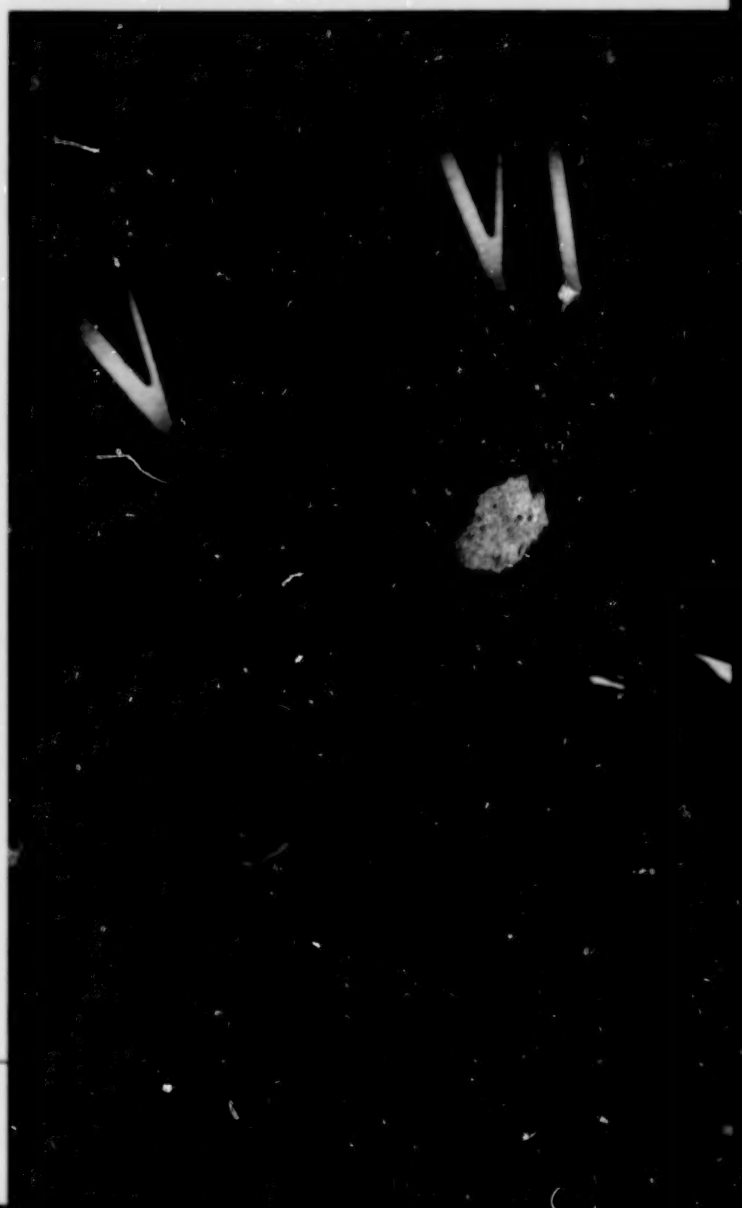
Neither the *1996 Act* nor the FCC's rules could foresee the rapid changes caused by these technological advances. Regulation, in short, struggled to keep up with the pace of technological advance in 1999. In sum, this relatively fluid regulatory and technological environment requires the NS/EP community to continually monitor and examine the implications on NS/EP telecommunications.

NETWORK CONVERGENCE

The continued enhancement of and adoption by industry and Government of Asynchronous Transfer Mode (ATM) and Internet Protocol (IP) networks stimulated speculation regarding the future of traditional circuit switched networks. AT&T's announcement that it will no longer purchase circuit-based switches further indicated a shift towards different transmission protocols.

Several corporate mergers (e.g., Lucent Technologies, Inc. and Ascend Communications; Nortel Networks, Inc. and Bay Networks) also foreshadow network convergence. Additionally, AT&T's planned acquisition of cable television company MediaOne Group, Inc. illustrates carrier efforts to establish themselves as full service providers of cable, Internet, and telephony. Altogether, these mergers reflect the telecommunications industry's belief that offering converged data and voice networking solutions is the way to secure future market shares.

The tremendous increase in use of the public Internet and expanding implementation of Intranet technology, including virtual networks, are strong indicators of the future direction of communications. However, much speculation surrounds the swiftness and extent of the shift. The lower levels of reliability and quality of data networks as compared with traditional voice networks hinder overall industry and Government confidence and, consequently, expeditious implementation of the next generation public network (PN). Additionally, the relative immaturity in enterprise management of data networks



compared to PN operations support systems poses a challenge that industry must overcome to promote interoperability of the divergent networks.

Maturation of data applications and technologies, such as improved quality of service offerings and the refinement of IP network-public switched network gateways and of data network enterprise management capabilities, will occur over the coming years. Additionally, true "one-stop shopping" network providers will likely emerge. These developments along with the economic and efficiency incentives associated with data networks could prompt expeditious multicarrier implementation of end-to-end next generation network technologies.

As network convergence occurs, the NS/EP community should continually examine opportunities for NS/EP services and operations.

Consequently, mission-critical NS/EP applications that rely on traditional networks may require reevaluation and renovation for use on data networks as convergence becomes prevalent.

YEAR 2000 TECHNOLOGY PROBLEM

During FY 1999, resolving the anticipated effect on automated networks of the Year 2000 (Y2K) problem remained a high priority for the Federal Government because our critical national infrastructures — including telecommunications, financial services, electric power, and transportation — rely heavily on information systems. Despite the efforts of each industry and all levels of Government to remediate their mission-critical information systems, every organization remained vulnerable to the disruption of its business processes because of the problems associated with Y2K. As Y2K approaches, concern remains about the vulnerability of our critical infrastructures to both domestic and international system failures.

In the telecommunications infrastructure, software is an essential component of the basic transport and switching facilities used for call completion. Consequently, the Y2K problem is of significant concern to the telecommunications industry and all those who depend on it, including Government entities with NS/EP responsibilities. Customer premises equipment and telecommunications services used to accomplish NS/EP missions have been under careful review and testing for Y2K compliance. As a result, the Y2K problem received a great deal of attention from telecommunications industry and Government managers. To ensure Y2K readiness, both interexchange and local exchange carriers conducted extensive interoperability testing. The results of these tests have been encouraging. Further, internetwork tests are under development for international gateways.

Given the obvious time constraints placed upon Y2K remediation efforts, the timely and free flow of Y2K readiness information to the public and among businesses, including competitors, has been an important aspect of the Nation's ability to address its Y2K needs. However, many

telecommunications companies were initially reluctant to disclose information related to their Y2K readiness due to the potential for legal complications that could result from disclosing data subsequently determined to be inaccurate.

Recognizing the urgency of Y2K remediation efforts, the President signed into law the Year 2000 Information and Readiness Disclosure Act (P.L. 105-271) on October 19, 1998. The law encourages information sharing by protecting from liability businesses that inadvertently share inaccurate information regarding their Y2K readiness.

As evidenced by the robust testing efforts over the past year, the United States telecommunications infrastructure will meet the millennium challenge. However, even the most painstaking remediation efforts cannot guarantee total eradication of the Y2K problem from networks or systems. Moreover, other Y2K preparedness issues warrant consideration. First, the Y2K problem is global. Although the United States is taking measures to deal with the problem, there is concern that carriers in other nations, especially those in developing countries, will not handle system failures caused by Y2K. Also, Y2K preparations indicate that the impact of the Y2K problem will transcend the January 1, 2000, roll over; it is a long-term problem, and disruptions and outages attributable to Y2K could occur well before or after the actual date change.

With these issues in mind, the Federal Government initiated an aggressive contingency planning effort to prepare for Y2K. Industry and Government representatives coordinated their Y2K preparations and established plans for responding to Y2K induced outages and maintaining Government NS/EP services. Multipath communications capabilities are in place to support coordination between Federal Government and telecommunications industry centers in the event of PN degradation. Such initiatives will help provide the telecommunications capabilities needed to keep NS/EP missions fully operational if PN outages occur. The Federal Government also worked to establish an international early warning system, providing the United States with up to 17 hours of advance warning of possible Y2K disruptions.

CRITICAL INFRASTRUCTURE PROTECTION

The conclusion of the Cold War, the success of coalition forces in the Persian Gulf War, and what President George H. W. Bush referred to as a "new world order" characterized the beginning of the 1990s. Yet, as the Cold War faded, new threats to the national interest emerged and captured the attention of the Federal Government. Today, the United States faces a more diffuse strategic environment than at any other point in its history, one increasingly characterized by nontraditional physical and cyber threats posed by nation-states, terrorists, criminal organizations, and other groups. Moreover, the potential targets of attacks have grown to encompass threats to our Nation's critical infrastructures, which support national security, economic competitiveness, and public safety and welfare.

Historically, our approach to protecting infrastructures was fragmented. Infrastructures were separately regulated and independent of one another, allowing for unique solutions to ensure their continued operation. However, three factors continue to alter how the United States views its infrastructures:

- There is a growing awareness of the extent to which the Nation depends on the information infrastructure and computer controlled networks to support the continued operation of all infrastructures

- Deregulation and globalization are forcing infrastructures to become more commercially efficient through adoption of information technology solutions

- Interdependencies among infrastructures exacerbate the potential consequences of growing threats and vulnerabilities.

To address the threats posed to and vulnerabilities of critical infrastructures,

President Clinton signed Presidential Decision Directive 63 (PDD-63) on May 22, 1998. PDD-63 directs the Federal Government to eliminate infrastructure vulnerabilities that our Nation's adversaries could exploit through physical or cyber means. To that end, the directive calls for an enhanced public-private partnership and creates several new structures to facilitate that partnership. It also designates a National Coordinator for Security, Infrastructure Protection, and Counter-terrorism to serve as a focal point for national critical infrastructure protection initiatives.

During FY 1999, the Federal Government undertook three broad initiatives to implement the provisions of PDD-63 across each infrastructure: 1) require Federal departments and agencies to develop internal plans for infrastructure protection; 2) promote industry efforts to implement Information Sharing and Analysis Centers (ISAC) within each infrastructure; and 3) develop a National Information Systems Protection Plan to coordinate the efforts of DOD, Federal departments and agencies, and the private sector to protect critical infrastructures from attacks and interruptions.

Today's security environment clearly warrants vigilance in the face of new threats. The bombings of the World Trade Center in New York, the Murrah Federal Building in Oklahoma City, and the U.S. embassies in Tanzania and Kenya, and other incidents over the past decade vividly remind us that physical threats to U.S. interests, both domestically and abroad, exist and can result in an enormous loss of life and property. Similarly, recent cyberattacks on Federal information systems and investigations of espionage at our national laboratories illustrate the value of computers as weapons in the Information Age and demonstrate how weaknesses in our computer and telecommunications networks expose the United States to new risks. For these reasons, addressing the threats and vulnerabilities affecting our critical national infrastructures is one of the most important challenges facing our Nation as we approach the 21st century.

EMERGENCY DISASTER RESPONSE

Diverse technological and national security vulnerabilities characterize today's NS/EP telecommunications environment. However, natural disasters also pose a real threat to the Nation's safety and security. Although sometimes viewed as at the lower end of the threat spectrum, natural disasters regularly exact high economic costs and can result in significant losses of life and property.

Natural disasters affect every U.S. State, varying in both form and severity. Large population centers on the East and West Coasts are susceptible to hurricanes and earthquakes, while disasters such as floods, fires, and tornadoes have the potential to strike anywhere in the Nation. The disruption and destruction wrought by natural disasters will continue to increase as our infrastructures grow in complexity and value. Federal mandates require robust NS/EP telecommunications capabilities, which provide a vital link in Federal response strategies by facilitating an immediate and coordinated response to emergencies, to enhance emergency preparedness and response and reduce disaster losses.

Manmade emergencies also constitute a serious threat to the Nation. Political unrest and war occurring in many parts of the world remain distinct threats to the security of the United States. Closer to home, there exists a credible threat of terrorist use of weapons of mass destruction. The possibility of a widespread disaster arising from the use of a nuclear, biological, or chemical agent is a serious and growing concern as indicated by recent policy on counter-terrorism such as Presidential Decision Directives 39 and 62, entitled "United States Policy on Counterterrorism" and "Combating Terrorism," respectively. The occurrence of any one of these events or other emergencies, such as a humanitarian aid effort abroad or a major transportation accident domestically, would necessitate an immediate and coordinated telecommunications support function or response.

FACING ISSUES OF THE 21st CENTURY

As the NCS prepares to enter the 21st Century, the strategic environment facing NS/EP telecommunications continues to change. For the first 25 years of its life, the NCS was primarily concerned with the military threats of the Cold War Era. As the Cold War ended, the NCS became more concerned with the effect that physical damage — caused by natural disasters and man made events, such as terrorist attacks — had on the availability of NS/EP telecommunications services.

Since the early 1990's, both the NCS and NSTAC have understood the importance of securing the computers and information systems that control and operate the Nation's telecommunications networks to assure the availability and reliability of NS/EP telecommunications service. As we better understand the interdependencies of all the Nation's critical infrastructures, the implications of a "cyber attack" on the telecommunications infrastructure takes on new meaning.

In responding to the Year 2000 technology problem, the NCS and the telecommunications industry have come to understand the importance of information sharing in assuring an adequate response to a potential crisis. Information sharing is also critical to a timely and effective response to a cyber attack on our critical infrastructures. As we move into 2000 and beyond, the OMNCS will continue working to build on the information sharing successes from Y2K in addressing the cyber threat to the Nation's NS/EP telecommunications system.

REPORT ORGANIZATION

Changes in the national security threat and the geopolitical environment, new developments in technology and the marketplace, and the vital importance of the telecommunications infrastructure to all sectors of the economy and society make the NCS's mission more critical than ever. The subsequent sections of this report highlight the NCS's FY 1999 activities and accomplishments undertaken to fulfill its mission.

Section II describes the emergency response activities of the OMNCS. Section III contains information on OMNCS Y2K preparation and contingency planning, plus a description of OMNCS NS/EP telecommunications support, activities, programs, and major interagency initiatives. Finally, Section IV reviews the NS/EP telecommunications support and activities of the NCS member organizations.

The *FY 1999 National Communications System Report* reflects the NCS's commitment to meeting the full range of NS/EP telecommunications needs for the Nation under all circumstances.

II

EMERGENCY RESPONSE ACTIVITIES

EMERGENCY RESPONSE ACTIVITIES

The National Communications System's (NCS) National Coordinating Center for Telecommunications (NCC) ensures that Federal, State, and local responders receive national security and emergency preparedness telecommunications support during disasters. The NCS also provides support to emergency response efforts through training of key personnel and provision of telecommunications resources.

The NCS provided communications support to disaster relief efforts in response to Hurricane Floyd during fiscal year (FY) 1999. During September 1999, the NCS deployed three augmentees to assist response crews in support of these disasters. Staff members were available throughout the disaster to provide emergency telecommunications resources as necessary. In addition, the NCS focused its FY 1999 support efforts on training and exercises to improve future disaster recovery response.

NCC 9/9/99 Y2K EMERGENCY OPERATIONS TEAM ACTIVATION

On September 8 and 9, the NCC conducted the first operational test of their year 2000 (Y2K) response capabilities. In preparation for the first of several critical Y2K-related dates, the NCC activated its emergency operations team for a 48-hour period. September 9, 1999 was a critical Y2K date because it was suspected some programs could mistake the "9999" date code for an end-of-file command sequence used in some software to bring certain processes to an end. This occurrence could have caused computer programs and equipment controlled by microprocessors to malfunction.

This test allowed the NCC, other Federal Government agencies, and participating telecommunications carriers to exchange Y2K information in real time and test the functionality of the NCC Y2K database. During this activation, the NCC received periodic network status information from 47 carriers in 29 countries via the Y2K database. Although there were

nodifficulties reported during the 9/9/99 rollover, participants benefited from the opportunity to share information about the status of their networks and tested their procedures for the millennium rollover. In addition to testing the Y2K database, NCC Y2K response plans were also tested and validated.

TELECOMMUNICATIONS EMERGENCY RESPONSE TRAINING

NCS Operations Planning and Support continued development of the third phase of the Telecommunications Emergency Response Training (ERT) seminars and targeted ERT sessions. Phase III seminars are planned to reach emergency responders and planners in the 10 Federal regions defined by the General Services Administration (GSA) and will be conducted nationwide beginning February 2000. These seminars are the third in a series of seminars designed to provide participants with information that can assist in providing telecommunications support to Presidentially declared emergencies and disasters. Phase III will offer information on emergency plans and activities in these critical areas: a) National resources including the Federal Response Plan (FRP), Emergency Support Function #2 - Communications (ESF #2), and NCC support; b) regional emergency operations and telecommunications services; c) national and regional emergency operations; and d) current and future technologies. A panel discussion on disaster and terrorist response operations and issues will also be conducted to familiarize participants with the responsibilities and requirements of responders across all levels of emergency operations.

The targeted ERTs, which are smaller and more informal than full ERTs, are geared specifically for newly appointed NCS Regional Managers and their staffs. These smaller sessions provide an opportunity for Regional Managers to receive one-on-one training and information on the programs and support the NCS offers during emergency response operations. Course content will vary depending on regional participant requirements. In addition to providing training, the seminars are designed to facilitate the development of working relationships among telecommunications emergency responders. The first targeted ERT was conducted in Federal Region III/Mid-Atlantic Region (Philadelphia) in July 1999. During FY 2000, a targeted ERT will be conducted in Federal Region IX/Pacific Rim Region. Region IX serves the States of Arizona, California, Hawaii, and Nevada; and the Territory of American Samoa, the Territory of Guam, the Commonwealth of the Northern Mariana Islands, the Republic of the Marshall Islands, the Federated States of Micronesia, and the Republic of Palau.

NCS REGIONAL MANAGERS CONFERENCE

NCS Operations Planning and Support, with support from the GSA, held a Regional Managers Conference for the Regional Emergency Communications Planners and the NCS augmentees in January 1999. Conference participants received detailed information about the evolving roles and responsibilities related to disaster planning and response operations in the 10 Federal Regions. The conference fulfilled the following objectives:

- Provided a forum for presenting NCS programs supporting the Federal Regions
- Established new goals and objectives for the expanding NCS regional role
- Identified regional support requirements for developing new planning procedures

▶ Ensured FRP ESF #2 roles and expectations were understood

▶ Prepared regionally assigned NCS augmentees for their 2-week active duty.

The conference was interactive, generating discussion among the Regional Managers and NCS augmentees on areas of common interest. It provided findings and recommendations to participants for future actions supporting and enhancing NCS mission readiness, such as planning, staffing, training, and exercise support.

NCS CONTINUITY OF OPERATIONS ORIENTATION

In November 1998, the NCS sponsored a continuity of operations orientation session and relocation site visits for NCC Emergency Operations Team members. The orientation provided an overview of the Continuity of Operations Plan, which was released earlier in the year, and the NCC Relocation Plan. It also served as preparation for two excursions to the NCC relocation site. The site visits enabled team members to familiarize themselves with the relocation facility, review their respective responsibilities, verify facility access procedures, and test NCS equipment. Participants also provided feedback on additional resources required within the NCS work area.

III

NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

NS/EP TELECOMMUNICATIONS SUPPORT, ACTIVITIES, AND PROGRAMS

This section highlights the activities and accomplishments of the Office of the Manager, National Communications System (OMNCS), the National Communications System (NCS), and the national security and emergency preparedness (NS/EP) community during fiscal year (FY) 1999. Special emphasis is given to OMNCS reorganization, its preparations related to the Year 2000 (Y2K) technology problem, and the telecommunications infrastructure. The introduction to this section recounts the evolution of OMNCS Y2K preparedness initiatives; the remainder of the section presents further details of OMNCS program-specific activities.

OMNCS REORGANIZATION

On September 1, 1999, OMNCS reorganized its divisional structure. The Manager, NCS, approved the OMNCS reorganization to improve the OMNCS focus on information assurance (IA) issues, consolidate IA resources, and create a strong IA presence at the National Coordinating Center for Telecommunications (NCC).

The major change was the merger of the Technology and Standards Division (N6) with the Programs Division (N2) to form the Technology and Programs Division (N2). This division assumes a majority of the IA activities held previously by the Customer Service and Information Assurance Division (N5). In addition, an Indications, Assessment and Warning (IAW) unit was established within the Operations Division (N3).

The Customer Service and Information Assurance Division (N5) was renamed the Customer Service Division.

OMNCS Y2K PREPAREDNESS ACTIVITIES

Early Awareness. In January 1998, the Manager, NCS, asked the President's National Security Telecommunications Advisory Committee (NSTAC) to provide a report to the President on the status of telecommunications industry actions to ensure continuity of service through the millennium transition. Although efforts to make the telecommunications infrastructure Y2K-ready were well under way,

the pervasive nature of the Y2K technology problem raised concerns about potentially unprecedented levels of degradation or inoperability within the infrastructure. In response to the Manager's request, the NSTAC recommended actions to the President to enhance the Y2K readiness of NS/EP telecommunications and to mitigate the impact of any Y2K-induced service disruptions on the Nation's NS/EP posture. In addition, the NSTAC's Industry Executive Subcommittee (IES), working in conjunction with the OMNCS, began to facilitate meetings between industry and Government to help ensure that all aspects of the Y2K problem pertaining to NS/EP telecommunications were considered and that appropriate contingency plans were developed.

Building on its industry/Government coordination role, the OMNCS became increasingly involved in high-visibility Y2K events and activities. In July 1998, the Deputy Manager, NCS, and the chair of the NSTAC's Network Group addressed the Senate Special Committee on the Y2K Technology Problem. Testimony focused on the actions OMNCS and NSTAC were taking to address Y2K readiness of NS/EP telecommunications services. Concurrently, the OMNCS became actively involved in the Network Reliability and Interoperability Council's (NRIC) efforts to address Y2K-related telecommunications issues. Rechartered in 1998 and chaired by AT&T's chief executive officer, the NRIC advises the Federal Communications Commission (FCC) on the efforts of the industry to prepare for Y2K conversion.

Growing Interest. High-level interest in OMNCS Y2K activities intensified as the Director, Office of Science and Technology Policy (OSTP), convened the Joint Telecommunications Resources Board (JTRB) on January 5, 1999, for the first time in more than 6 years. Established to provide advice to the Director, OSTP, in the exercise of the Director's nonwartime telecommunications functions assigned by Executive Order (E.O.) 12472, the role of the JTRB is to provide advice and guidance on telecommunications matters to the President and Federal departments and agencies. Senior representatives from the Department of State (DOS), Department of Defense (DOD), Federal Emergency Management Agency (FEMA), the General Services Administration (GSA), the National Telecommunications and Information Administration, the FCC, and the NCS met in the Old Executive Office Building to discuss general Y2K issues and the role of the JTRB during any Y2K crisis. As a result of this first meeting, the NCS agreed to provide the OSTP with a recommendation whether to convene the JTRB in the wake of a disruption in telecommunications services during the rollover. A follow-up meeting on August 5, 1999, addressed specific response and coordination issues through the use of scenarios created by the OMNCS.

The OMNCS had undertaken significant research before January 1999, to determine the potential effects of Y2K on the public switched network (PSN). Initial efforts included gathering data on telecommunications equipment compliance. Switch failure was of great concern to commercial and Government sectors. Definitive data had not been gathered to construct a model that would project effects on the critical user community and potential national security implications. Therefore, at an NCS Council of Representatives (COR) meeting in late January 1999, the OMNCS requested key facility data from each member agency. By obtaining this crucial information, the OMNCS was able to outline areas of concern where Y2K-induced failures could occur.

Expanding National and International Participation. The long-standing role of the NCC in coordinating industry/Government telecommunications responses and NCC's potential value during the Y2K rollover brought a number of industry/Government organizations to the NCC to discuss mutual Y2K response issues. At the

same time, the OMNCS conducted an extensive data collection effort to identify the Y2K compliance of telecommunications assets that support critical Government facilities. This information was shared with each of the member agencies to aid in the preparation for Y2K.

In early 1999, the U.S. Government began to voice concern about the possibility of a Y2K-induced incident that could induce a domino effect across critical infrastructures. Countries west of the international dateline would first witness the effect. Realizing that prompt action was essential, the OMNCS began development of an early warning mechanism to enable efficient preparedness within the response community. Cooperation between industry and Government, both domestically and internationally, would be essential to this initiative.

Initially, the companies in the telecommunications industry had been preparing for the potential effects of Y2K individually, concerned predominantly with company operations rather than the national network of telecommunications assets. Although individual companies were providing customer-oriented solutions, an infrastructure-wide effort was lacking.

Concerned with the potential ramifications of a widespread outage, the Telco Y2K Forum decided to create a data repository of incident information. The Telco Y2K Forum, which includes representatives from the largest local domestic carriers in the United States, was formed in 1996 to share information and promote participation in Y2K testing initiatives. During a meeting between the Telco Y2K Forum and the NCS in February 1999, the Manager, NCC, and Forum representatives agreed that the OMNCS would lead an effort to create an incident database. This database would store incident information enabling awareness of potential events for critical users. The Forum felt it was in the best interest of its members to share real-time network and equipment data with the OMNCS. By doing so, potential problems could be identified early, response would be decisive, and results would be shared in an effort to preempt failures in networks throughout the United States. The outcome of this agreement was the NCC Y2K database, which would correlate input from trouble reports, allow participating members access to these reports, and produce pattern analysis reports to aid Y2K response efforts.

The OMNCS proceeded to secure participation in the database effort among domestic telecommunications carriers and vendors to provide early warnings domestically. However, because the telecommunications infrastructure does not exist solely as a domestic entity, it was imperative for the OMNCS to secure international participation as well. During a meeting of the North Atlantic Treaty Organization (NATO) Civil Communications Planning Committee (CCPC), Stockholm, Sweden, in March 1999, the Manager, NCC, articulated the significance of creating an early warning mechanism. The Manager also briefed NATO's Partnership for Peace on NCS/NCC Y2K changeover plans at that time.

In April 1999, the NCS held negotiations with Canada and several International Telecommunication Union (ITU) members in a move to foster international cooperation. An agreement was reached that would allow international entities to share data. The NCC Y2K database would therefore serve as a mechanism to provide the OMNCS with international data necessary to successfully produce early warning messages, alert international members through advisories, and supply possible solutions to problems occurring in similar equipment types.

To further assist in the information-sharing process, the OMNCS expanded its External Affairs home page during FY 1999 to include a separate section on Y2K activities. The Y2K home page provides information on OMNCS Y2K activities, links Web customers to other Government Y2K program Web sites, and provides a source of news articles and speeches from senior Government officials on Y2K issues.

Preparation, Coordination, and Implementation. The Y2K Information Coordination Center (ICC), established by the President's Y2K Conversion Council to provide the President with an accurate, unified picture of the Y2K status of the Nation during Y2K rollover periods, contacted the NCC in April 1999, to discuss the use of the industry-provided information in the NCC Y2K database to support the ICC mission. It was agreed that the NCC would play a major role in providing regular national telecommunications infrastructure status incident reports and assessments to the ICC.

In addition to its central role in maintaining the telecommunications Y2K database, the OMNCS worked to ensure that its NS/EP telecommunications programs, including the Government Emergency Telecommunications Service (GETS), the Shared Resources (SHARES) Program, and the Telecommunications Service Priority (TSP) System, were prepared for Y2K. The GETS program, providing nationwide voice band service for authorized Government users engaged in NS/EP missions, supplied more than 6,500 personal identification numbers (PIN) to key personnel in Federal, State and local agencies as part of a plan to address potential Y2K failures.

The SHARES program prepared to provide a backup means of communications through the use of high frequency (HF) radios should the public network (PN) be significantly degraded. Several Federal agencies have declared SHARES and HF radios as the primary backup communications media for their Y2K and Continuity of Operations (COOP) plans. During the rollover period, SHARES will increase their operational readiness to Level One, the highest degree of preparedness, in the event of confirmed PN outages.

The TSP System experienced an increase in requests from NCS member agencies for service prioritization. Requests were made to promote quicker vendor response times to critical circuits potentially affected by Y2K. Additionally, the TSP System's primary server, the Priority Telecommunications System, was tested for potential date anomalies to ensure continuity of operations during the Y2K transition. The tests confirmed that all critical hardware and software is indeed Y2K-compliant.

In addition, the OMNCS also focused on enhancing the National Telecommunications Coordinating Network (NTCN). The NTCN ensures coordinated communications among key Federal departments and agencies, telecommunications carriers, and equipment manufacturers during periods of potentially widespread PN outages caused by Y2K. To guarantee NTCN operation during the Y2K rollover period, the NCC implemented a number of enhancements to the existing system and installed a duplicate system at the NCC relocation site. System enhancements included purchasing and installing a conference bridge for each system. This conference bridge interconnects various types of communications systems enabling the users to communicate between different types of media. This connectivity is crucial between telecommunications industry representatives and Y2K mission-critical Federal departments and agencies. Finally, the NCC conducted NTCN training of operators and users and performed a system validation to ensure system readiness.

To coordinate their expanding Y2K response role and to ensure their Y2K readiness, the OMNCS and the NCC developed a industry/Government Y2K Operations Plan. The NCC published the first version on May 19, 1999, and continued to expand, update, refine, and coordinate the document throughout the year. Designed as a living document, the plan provided a record of NCC preparedness and Y2K compliance activities. It also provided organizations with a ready reference on NCC operational information to enhance the interoperability of organizational contingency plans with the NCC.

Additionally, the OMNCS, along with the NCC, sponsored a series of Y2K training events for Emergency Operations Team (EOT) members and other NCS personnel. These seminars provided participants with information about Y2K issues, particularly as they apply to NCC

response operations. The first seminar, held in April 1999, provided participants with introductory and background information on Y2K topics and industry/Government preparations. The second session, held in May, focused on emergency response tools and resources for NCC Y2K rollover operations. This seminar described the Y2K compliance of infrastructure-related systems within the NCC operations center, the Defense Information Systems Agency (DISA) headquarters building, and the NCC relocation site. The final seminar in August detailed the preparations for NCC Y2K operations. This session provided demonstrations and hands-on experience with some of the NCC's response equipment. Subject matter experts invited by the OMNCS conducted each of these seminars.

To supplement these training seminars, Training, Exercise and Regional Support (TERS) supported FEMA in the development of a series of Y2K tabletop exercises. These exercises included the following:

- **FEMA Y2K Tabletop Exercises** were held in February and March 1999. These seminars were designed for members of each FEMA region's Regional Interagency Steering Committee (RISC).

- **FRP Community Y2K Tabletop Exercise** was held in May 1999, following the Regional Y2K Workshops. This event was designed to explore issues related to supporting Federal consequence management response resulting from Y2K.

- **National Y2K Tabletop Exercise** was attended by designated White House officials, Cabinet Secretaries, and other designated senior U.S. Government officials. The National Y2K Tabletop Exercise reviewed U.S. policies for international and domestic consequence management and project leadership and focused on coordination among departments and agencies, identification of potential issues, and enhancement of participants' ability to respond in a Y2K environment.

By June 1, implementation of the NCC Y2K Database and its support structure was nearly completed as final additions to the database were made, and the development of training, test, and evaluation plans, procedures, and exercises was well under way. The beta version of the database was put on line on July 1, 1999, and industry and Government participants began user familiarization and testing. Close coordination was maintained with all participants to encourage feedback on database performance. On July 13, the OMNCS established the Y2K Configuration Control Board to work closely with users and developers to evaluate all additional database requirements and proposed changes. On July 29 and 30, the OMNCS sponsored Y2K Database administrator training for industry and Government users from all over the country. The focus of the training was to ensure all users had a common understanding of database information fields and operational features. The high point of the implementation phase was an industry/Government database test on August 18, 1999.

Online and Ready. On August 18, the operational database was put on line and tested, and the NCC focused on preparations for the critical Y2K rollover date on September 9. Programmers have used "9999" as the end of file command for a number of programs to signify termination of these programs. It was feared that computers would misinterpret the "9/9/99" date as this end of file command. This misinterpretation by computers could cause the computer program to terminate and could create potential outages during rollover. The NCC activated its EOT and went on full alert for the period September 8–9, 1999. This activation allowed a dress rehearsal for industry and Government participants before the most critical Y2K date of January 1, 2000. The NCC and its industry and Government partners proved that they would be ready.

TECHNOLOGY AND PROGRAMS

The Technology and Programs Division implements evolutionary telecommunications NS/EP capabilities for an enduring and effective telecommunications infrastructure. The division develops technical studies, analyses, and standards that promote the reliability, security, and interoperability of NS/EP telecommunications.

Objectives emphasize incorporating advanced, cost-effective technology into NS/EP communications programs. In fulfilling this mission, division personnel evaluate emerging technologies to mitigate technical impediments to interoperability and satisfy NS/EP requirements. They use this information as they participate in industry and international standards organization meetings to ensure that NS/EP requirements are incorporated in the standards and recommendations developed.

The following paragraphs highlight the major projects undertaken by the Technology and Programs Division during FY 1999.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE

BACKGROUND

The OMNCS established GETS to meet White House requirements for a survivable, interoperable, nationwide voice band service for authorized Government users engaged in NS/EP missions. GETS satisfies these requirements by providing emergency access and specialized processing in local and long-distance telephone networks. GETS ensures users a high rate of successful call completion during network congestion or outages arising from natural or manmade disasters.

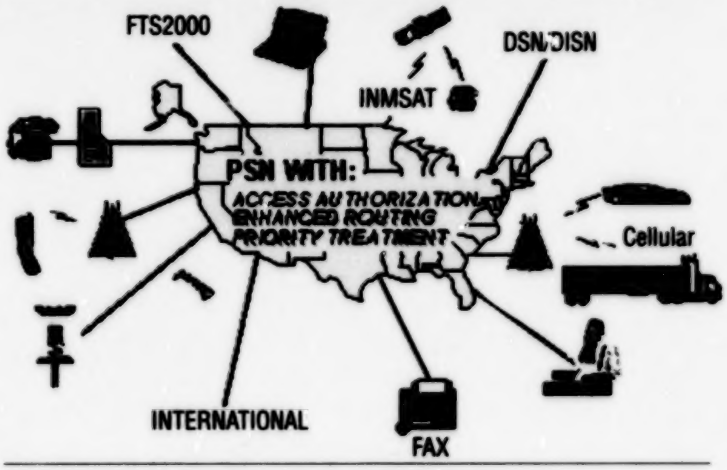
From the beginning, GETS planners focused on the PSN as the most efficient, reliable technology for supporting a service that would meet NS/EP mission requirements. The use of the PSN leverages the PSN's vast resources — a $300 billion infrastructure with more than 170 million access lines, 26,000 switches, and 2,200 mobile switching centers. The PSN is ubiquitous, robust, and flexible. It supports 95 percent of the Government's telecommunications needs, and despite its enormous size and complexity, the PSN averages 99.999 percent availability.

Exhibit 3-1 shows the various means of communications through which GETS users can access the system.

The initial objective of GETS planners was to expeditiously field a service that would provide priority call treatment and then incrementally improve the service with specialized calling features. The strategy of developing GETS by using the existing assets of the PSN enabled early implementation and provided for technical currency by leveraging the continual improvements made by the industry. Using the software resources of the PSN also made it unnecessary for the Government to purchase, install, maintain, and eventually update network equipment.

Exhibit 3-1

GETS Operational Concept



The approach to implementing GETS initially focused on the interexchange carrier (IXC) portion of the network. This approach resulted in separate GETS contracts with AT&T, MCIWorldCom, and

Sprint — the three largest IXCs. As a result, these carriers are the only IXCs capable of authorizing and processing GETS calls. Therefore, it is critical that access to these carriers be available at all PSN end offices and mobile switching centers. Each of these IXCs began with the same basic set of functional requirements; however, as a result of the implementation approach pursued by each IXC and the inherent differences in the structure of their respective networks, the operational features and capabilities differ slightly among the providers.

Today, the primary focus of feature implementation has shifted to the local exchange carrier (LEC) networks. A separate integration contract (IC) was competitively awarded to GTE Government Systems Division for integration of LEC implementation of GETS and for overall GETS operation, administration, and maintenance services. The first phase of GETS LEC feature deployment, alternate carrier routing (ACR), was based on advanced intelligent network (AIN) technology. ACR enhances access by automatically attempting all three GETS IXCs. The GETS IC entered into contracts with four primary switch manufacturers—Lucent, Nortel, AG Communications Systems (AGCS), and Siemens for the implementation of priority treatment and enhanced routing features on their products. The GETS IC also entered into contracts with LECs for the deployment and operation of these features. During FY 1999, deployment of features began in several LECs on Nortel, Lucent, and AGCS switches.

The OMNCS also is investigating potential enhancements in other areas of the PSN. The GETS IC, through a contract with Lucent, conducted a demonstration of potential cellular network enhancements that initiated a dialogue with industry on what should be done to enhance NS/EP telecommunications in the wireless networks. Based on proposals by the switch vendors that leverage recently completed LEC feature development, the GETS Program is investigating enhancements that would help GETS calls terminate from the PSN to customer premises (e.g., private branch exchanges [PBX]). The GETS Program also continues to monitor the potential impact of opportunities offered by evolving network technologies, such as industry's recent movement toward offering voice service as a packet-based service.

The OMNCS created a phased implementation approach for GETS to accommodate the dynamic nature of the implementation effort. This approach has proven to be quite successful. The phases, designated Limited Capability (LC), Initial Operational Capability (IOC), and Full Operational Capability (FOC), are described briefly below.

- The **LC phase** began on September 30, 1994. Throughout this phase, users were able to place GETS calls through the LECs, using the universal GETS access number, to the three IXCs that provide GETS priority call processing. During this phase, implementation of additional features took place on the IXCs, to include interoperability with Federal Telecommunications System 2000 (FTS-2000), Diplomatic Telecommunications Service, and the Defense Switched Network.

- The **IOC phase** began on October 1, 1995. IOC capabilities consist of all LC capabilities and additional IXC services. The GETS services in the LECs consisted of the initial deployment of alternative carrier routing.

- The **FOC phase** is scheduled for the year 2001. FOC capabilities will include all IOC capabilities as well as LEC network features currently in place or under implementation. During this phase, additional capabilities may be implemented based on analyses that demonstrate the benefit of such capabilities.

OPERATION AND FEATURES

Access to GETS is quick and simple. Users access GETS by dialing a universal access number (1-710-NCS-GETS) using common telephone equipment, such as a standard desk set, secure telephone (e.g., STU-III), facsimile, modem, or cellular phone. Telephones on the FTS-2000 Network, the Diplomatic

Telecommunications Service, and the Defense Information Systems Network (DISN) can also access GETS.

When the GETS access number is dialed, a tone prompts the user to enter a Personal Identification Number (PIN) and the destination telephone number. Even if the access control system fails, there is a "fail open" feature that will allow authorized users to complete their GETS calls. The OMNCS can deactivate PINs for fraud or abuse.

PRIORITY TREATMENT AVAILABILITY

In addition to implementing priority treatment and enhanced routing features in the IXC and LEC trunk networks, the OMNCS is also working to ensure NS/EP calls receive priority in the Signaling System 7 (SS7) networks that manage calls in the carrier trunk networks. In 1993, the American National Standards Institute (ANSI) approved the High Probability of Completion (HPC) Standard ANSI T1.631-1993 that provides both a classmark for NS/EP-related signaling messages and a high priority level for those messages within the SS7 message priority scheme. The classmark allows NS/EP calls to be recognized in any network, facilitating the application of available GETS features. The higher priority level was designed to improve the likelihood that GETS calls would continue to be processed in the event of congestion within the SS7 networks.

In 1996, ANSI modified the SS7 standards so that NS/EP traffic would not share the higher priority level with plain old telephone service (POTS) traffic. The GETS Program worked closely with the Network Interconnection and Interoperability Forum (NIIF) to facilitate industry migration to the 1996 standard related to SS7 message priority. GETS representatives worked with NIIF members to build consensus on a migration plan and schedule and won adoption of a resolution codifying the plan. NIIF introduced Issue No. 0095, *Implementing POTS IAM Priority Level 0*, in December 1997. Based on the resolution, plans have been received from most members providing specific dates by which they will comply with the standard. Plans are expected to be provided by the remaining members early in FY 2000.

The switches that either currently comply, or will soon have the capability to comply, with the standard will serve more than 90 percent of the access lines in the country.

INTEROPERABILITY

Many of the significant challenges currently facing GETS involve consistent toll-free treatment for service users at privately owned user-to-network access devices. Similar to other services, GETS must navigate the new services-rich, but highly competitive, telecommunications environment spawned by the *Telecommunications Act of 1996*. Resulting industry deregulation has led to a significant increase in the number of service providers within the industry. This environment has given rise to difficulties in placing successful toll-free GETS calls from privately owned point-of-exchange devices, such as coin phones and PBXs in some service areas. Testing has shown this to be particularly true for coin phones owned and operated by small businesses and PBXs operated by the hospitality industry (e.g., hotels and motels). Commonly encountered problems include the requirement to deposit coins at a coin phone before dialing, improper charging by hotel and motel billing systems, and the inaccessibility of GETS IXCs because of business arrangements between user-to-network device owners and IXCs.

Paramount to the problem of toll-free access at privately owned devices is industry recognition of the 710 Numbering Plan Area (NPA) as nongeographic, emergency, and toll-free. To this end, the OMNCS is working with the North American Numbering Plan Administrator (NANPA) and the FCC to issue guidance to industry on publicizing the 710 NPA to give it stature as an emergency toll-free service per Sections 228(c) and 276(b) of the Communications Act. Based on this work, the NANPA issued a planning letter (PL-NANP-172, April 12, 1999) advising industry of the Government's use of the 710 NPA. This letter

also notified owners and managers responsible for user-to-network access (including cellular/personal communications services [PCS] networks, PBXs, and payphones) of the need to ensure that 710 calls are not blocked by their equipment. Also, Telcordia (formerly known as Bellcore) modified the Local Exchange Routing Guide to include routing procedures for 710 calls.

In addition, the OMNCS is working with coin phone industry groups, such as the American Public Communications Council and hospitality industry organizations and associations, to raise awareness of GETS as an emergency, toll-free service to be given treatment similar to that provided for 911 emergency, toll-free calls.

SUCCESSES

In addition to being used to overcome congestion and damage associated with natural disasters, GETS was used to overcome a network failure in FTS-2000. In one instance, FTS-2000 calls could not be completed from Washington to Denver because of a failed switch. Government users were administratively blocked from using carriers other than FTS-2000 but were able to access GETS and complete their calls.

In the past year the GETS Program made significant progress in its outreach efforts to State and local user groups. The number of State and local agencies (including the American Red Cross) with GETS accounts rose from 121 to 177. State and local users now account for 5,364 of the more than 27,000 distributed GETS PINs.

NS/EP COMMUNICATIONS OVER THE INTERNET

Work has begun to assess the impact of using the Internet for NS/EP communications. While few critical NS/EP communications are carried by the Internet at present, increased use is expected. In addition, it is expected that many voice connections in the public networks (PN) will be transported by Internet-type data protocols. The areas that are being investigated include methods of obtaining NS/EP-specific priority services on the Internet, impact of switched and data network convergence on NS/EP services (e.g., GETS and TSP), and security of the Internet.

ADVANCED INTELLIGENT NETWORK

The AIN is a rapidly evolving telecommunications technology identified by the President's NSTAC and the OMNCS as potentially having the ability to meet the NS/EP telecommunications needs of NCS member organizations.

AIN technology supports the telecommunications architecture consisting of signaling systems, switches, computer processors, databases, and transmission media. The convergence of these elements allows for customized software-defined network services that can be flexibly, rapidly, and cost-effectively configured to meet changing customer needs. Among other capabilities, AIN provides priority recognition, user authentication, enhanced routing, and network management alternatives in support of NS/EP contingency operations.

In the competitive market environment created by the *Telecommunications Act of 1996*, PN carriers are becoming increasingly dependent on AIN capabilities to deliver services to their customers. Carriers are using AIN to deploy local number portability (LNP), as mandated by the FCC, to open networks to competitive service providers, and to meet customer demand for new service capabilities (e.g., mobility, data, internet access).

The AIN efforts in the OMNCS address AIN-based technology applications for NS/EP with the following mission objectives:

- Assess AIN architectures, standards, and implementations

- Define, develop, and demonstrate AIN NS/EP applications
- Ensure NS/EP requirements influence the evolving AIN technology
- Facilitate integration into Government initiatives (e.g., GETS, DISN)
- Evaluate AIN security, survivability, reliability, and interoperability.

The OMNCS coordinates with industry and NCS member organizations to fulfill mission objectives and to identify preliminary services that the OMNCS can introduce into NS/EP initiatives (e.g., GETS) through successful proof-of-concept demonstrations.

The OMNCS is deploying AIN-based alternate carrier routing to support LEC-enhanced routing. In conjunction with AIN efforts, the GETS Program Office is also pursuing use of the SS7-based HPC ANSI standard for further enhancements. Additionally, the OMNCS is investigating recent signaling network outages of AIN and SS7 network service providers.

Intelligent network capabilities have reached a critical mass in the public telecommunications network. The industry's deployment of LNP promises near-universal AIN availability. The OMNCS continues to monitor FCC rulemakings that may affect AIN availability and participates in industry forums to communicate NS/EP needs. Recent accomplishments include demonstration of an intelligent network-based release-to-pivot capability for efficient routing, analyses of intelligent network and network convergence issues, and a study of AIN signaling message priorities used to support GETS alternate carrier routing queries.

Currently, the OMNCS is evaluating the role of traditional intelligent network capabilities in emerging multimedia networks, intelligent devices, and future applications of the emerging wireless intelligent network. This applied research enables the AIN Program Office to influence these promising new technologies in the developmental stages and ensure the continued efficacy of existing and future intelligent network applications.

WIRELESS SERVICES

E.O. 12472 assigns the OMNCS the responsibility of conducting technical studies or analyses and examining research and development (R&D) programs to identify improved approaches that may assist Federal entities in fulfilling NS/EP telecommunications objectives. To carry out this responsibility, the OMNCS began several wireless program initiatives to ensure that industry understands NS/EP user requirements and supports these requirements in their networks.

CELLULAR PRIORITY SERVICE

Cellular Priority Service (CPS) is being accomplished in response to White House direction resulting from NSTAC recommendations. Natural disasters have repeatedly illustrated the importance of cellular technology in providing timely emergency telecommunications for Federal, State, and local users at a disaster site. However, increased personal use of cellular communications often creates network congestion and high levels of call blocking precisely when disaster relief officials most need mobile communications. As a result, the OMNCS, working with industry leaders, industry associations, State representatives, and standards bodies, developed the CPS Program to facilitate and coordinate the development of a cost-effective, uniform, nationwide cellular priority access service capability that enhances NS/EP user access to the PN.

The OMNCS is working with the FCC to address the regulatory issues associated with the implementation of cellular priority. In the meantime, the OMNCS has completed several studies investigating the technical aspects of CPS implementation.

ENHANCED SATELLITE CAPABILITY

Through the ESC Program, the OMNCS

investigates emerging satellite technologies, analyzes their ability to support NS/EP requirements, and works to improve and enhance their ability to support these requirements. The recent deployment of commercial low Earth orbiting satellite systems (e.g., Globalstar, ICO) created another potential source of NS/EP telecommunications.

WIRELESS DATA SERVICES

New technologies in the field of wireless telecommunications, beyond cellular and satellite technologies, continue to emerge. To investigate the potential of these technologies for providing NS/EP telecommunications, the OMNCS developed the Priority Wireless Data Services(PWDS) initiative.

Major areas being investigated to determine whether they can aid NS/EP users in successfully completing their missions are PCS, wireless data technologies, and unmanned aerial vehicles. As other technologies or systems develop, the PWDS Program will also examine these to ensure that the OMNCS remains aware of all relevant developments in telecommunications.

Wireless Data. The OMNCS continues to investigate wireless data technologies and service providers to identify potential support for NS/EP users, and to enhance Government awareness of wireless data capabilities. Delivery of these services can be via personal data assistants (PDAs) and cellular phones.

Unmanned Aerial Vehicles. A study was conducted to identify opportunities in the aerial platform technology industry to be used for NS/EP requirements. It was found that mounting a communications relay on an aerial platform would improve the communications range of any of the terrestrial-based systems. This technology would also allow Government agencies to use existing equipment.

Of particular interest to the NCS are high altitude platform stations (HAPS). A HAPS is a helium-filled, lighter than air platform with a telecommunications payload that may provide International Mobile Telecommunications (IMT)-2000 communications.

International Mobile Telecommunications-2000. IMT-2000 is an ITU initiative that uses a "family of systems" concept to unify the existing diverse wireless systems into an interoperable global infrastructure capable of offering a wide range of services, including global roaming. The OMNCS is determining the implications of IMT-2000 for NS/EP telecommunications. The OMNCS anticipates that IMT-2000 will mature around the year 2000.

Federal Wireless Users Forum. The Federal Wireless Users Forum (FWUF) provides an opportunity for current and future Government users of wireless services to obtain information on various types of services. The OMNCS facilitates the FWUF, focusing on technical issues and policies having implications for NS/EP telecommunications. The FWUF, the Federal Wireless Policy Committee, and the OMNCS co-hosted a workshop in May 1999. The workshop addressed regulatory issues, Federal user wireless requirements, wireless priority access, industry update on Y2K, wireless security issues, commercial wireless services, PCS, cellular, third generation wireless services, wireless data services, mobile satellite services, and DOD wireless issues. Representatives from Federal, State, and local governments, wireless equipment manufacturers, and service providers attended the workshop.

Personal Communications Services. Major OMNCS efforts focus on standardizing the Stage 2 service description for Priority Access and Channel Assignment-Enhanced (PACA-E) service. The Stage 2 description depicts the network architectures and message flows needed to implement the PACA-E service and describes how the various network entities interact to provide the service. This Stage 2 document is defining a new feature, PACA-E egress, which defines how a call attempt is queued on the egress side of the network. When finished, service providers can use it to implement queuing on the

egress side of their networks.

The OMNCS also actively participates in joint projects between the Telecommunications Industry Association committee TR45 and T1P1 concerning Enhanced Wireless Emergency Services. When developed, these standards will include location services and congestion control.

Land Mobile Radio. Land mobile radio (LMR) is a critical component of NS/EP communications. It is the common denominator for Federal, State, and local government personnel responsible for providing on-site support for NS/EP events. LMR, also called dispatch mobile radio, is widely used within every Government department and agency and is particularly valuable in NS/EP operations.

The OMNCS is a key participant in national and international standardization efforts for digital narrowband LMR, including the joint Federal, State, and local government standards effort called Project 25.

MULTIMEDIA

OMNCS personnel actively participate in developing national standards and international recommendations for multimedia service definition and multimedia systems, including the associated protocols, signal processing, terminals, and modems.

HIGH SPEED NETWORKS

Network Management. OMNCS personnel serve in leadership positions for the development of standards for high-speed networks. There has been a particular focus on developing a new family of international standards for online automation of network management operations and data interchange between commercial telecommunications service providers and their customers. This work is being conducted in the ITU Telecommunication Standardization Sector Study Group 4, Telecommunications Network Management and Network Maintenance. In addition, the international consortium known as the Network Management Forum, the ANSI T1M1 standards committee, and the U.S. Electronic Communications Implementation Committee also work on many critical issues that affect the standards being developed. These standards will bring automation to the network management processes and enable real-time interchange of management data.

Networks Physical Protection Standards. The OMNCS has worked to develop physical protection standards for the telecommunications infrastructure through ANSI and the ITU. Most recent efforts focused on ANSI T1.320-1994, which addresses practical cost-effective electrical protection techniques for telecommunications central offices.

Asynchronous Transfer Mode. The OMNCS is interested in understanding emerging uses for asynchronous transfer mode (ATM) and their possible application to NS/EP. Recent activities have focused on analyzing the application of ATM over asymmetric digital subscriber line (ADSL) systems and the relationships of popular transmission characteristics to perceived quality for digital video over ATM.

Dense Wave Division Multiplexing. The adoption of emerging dense wave division multiplex (DWDM) technology by IECs, LECs, and private enterprise networks reflects the initial phase in creating an all-optical broadband network. This network will have the high-speed network capabilities to meet the broadband demands of the evolving Internet, including the Internet's integration with telecommunications networks such as the public switched network (PSN).

Given all of the above factors, DWDM technology has potential NS/EP applications. Major OMNCS efforts focus on the analysis of DWDM technology to support crisis management and disaster communications; DWDM interoperability, interconnection, and interworking; and technical contributions for

incorporation of NS/EP interests into evolving optical transport network recommendation developments of the ITU's Telecommunication Standardization Sector, Study Group 13. Study Group 13 is responsible for general network aspects and studies relating to the initial studies of the impact of new system concepts and innovative technologies on telecommunication networks.

FEDERAL TELECOMMUNICATIONS STANDARDS COMMITTEE

In concert with its technology activities, the OMNCS manages the Federal Telecommunications Standards Program. This program develops NS/EP-related standards and recommendations through the Federal Telecommunications Standards Committee (FTSC) and through commercial, national, and international organizations. Established in 1972, the governmental interagency FTSC is chaired by the Chief of the Technology and Programs Division.

NETWORK MODELING AND ANALYSIS

OMNCS automated network modeling and analysis tools reside in the Network Design and Analysis Center (NDAC). The NDAC supports several OMNCS network reliability and IA activities and initiatives through telecommunications network modeling and analysis. A continuing objective is to maintain a current and valid data model of the U.S. PN. OMNCS personnel, with contractor support, continued to adapt current models to changes in PN architectures and routing schemes arising from the introduction of new carriers, networks, and technologies, such as synchronous optical networks, ATM, wireless services, and the Internet.

STRATEGIC ARCHITECTURE

The Technology and Programs Division develops a strategic architecture that defines future capabilities to fulfill NS/EP requirements. The architecture is a melding of requirements, developed by the Customer Service Division, with forward-looking, commercially standardized products and services.

FY 1999 PRODUCTS

Exhibits 3-2 and 3-3 present highlights of significant accomplishments in the Technology and Programs area. Exhibit 3-2 lists technical notes and technical information bulletins prepared by the Technology and Programs Division for member organizations and other Government agencies. Exhibit 3-3 lists Federal Telecommunications Recommendations (FTR) developed by the FTSC.

OPERATIONS

The Operations Division ensures the availability of telecommunications across the entire spectrum of emergencies. The following paragraphs describe activities of the Operations Division during FY 1999.

NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS

The NCC continues to serve as the operations focal point for the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities. Activity increased significantly as the NCC focused on Y2K issues and the enhancement of its indications, assessment, and warning (IAW) capability. NCC Y2K activities are discussed in the "Y2K Preparedness" portion of this document.

On October 15, 1998, the NCC IAW Center Pilot was concluded. It proved that the NCC could successfully conduct indications,

Exhibit 3-2

Technical Notes and Information Bulletins

Title	Date	Number
Channel Reservation vs. PACA Queuing: A Comparison of Priority Call Handling Techniques	January 1999	TN Vol. 6, No. 1
CORBA - A Prospective Solution to Interoperability	October 1998	TN Vol. 5, No. 3
Asynchronous Transfer Mode (ATM) Over Asymmetric Digital Subscriber Line (ADSL) Systems	January 1999	TIB-99-1
Relationships of Popular Transmission Characteristics to Perceived Quality for Digital Video Over ATM	January 1999	TIB-99-2
Gigabit Networking	January 1999	TIB-99-3
Telecommunications Network Time Synchronization	April 1999	TIB-99-4

Exhibit 3-3

Federal Telecommunications Recommendations

Title	Date	Number
Video Teleconferencing Services at 56 to 1,920 kbit/s	October 1998	FTR 1080A-1998

assessment and warning operations. The planning and implementation of enhancements to the NCC's IAW capability continue and will result in several new developments. These changes will include a revised industry/Government concept of operations; implementation of a training program for NCC staff; and additional operational capabilities to receive and correlate intrusion incident data feeds from industry/Government operations centers.

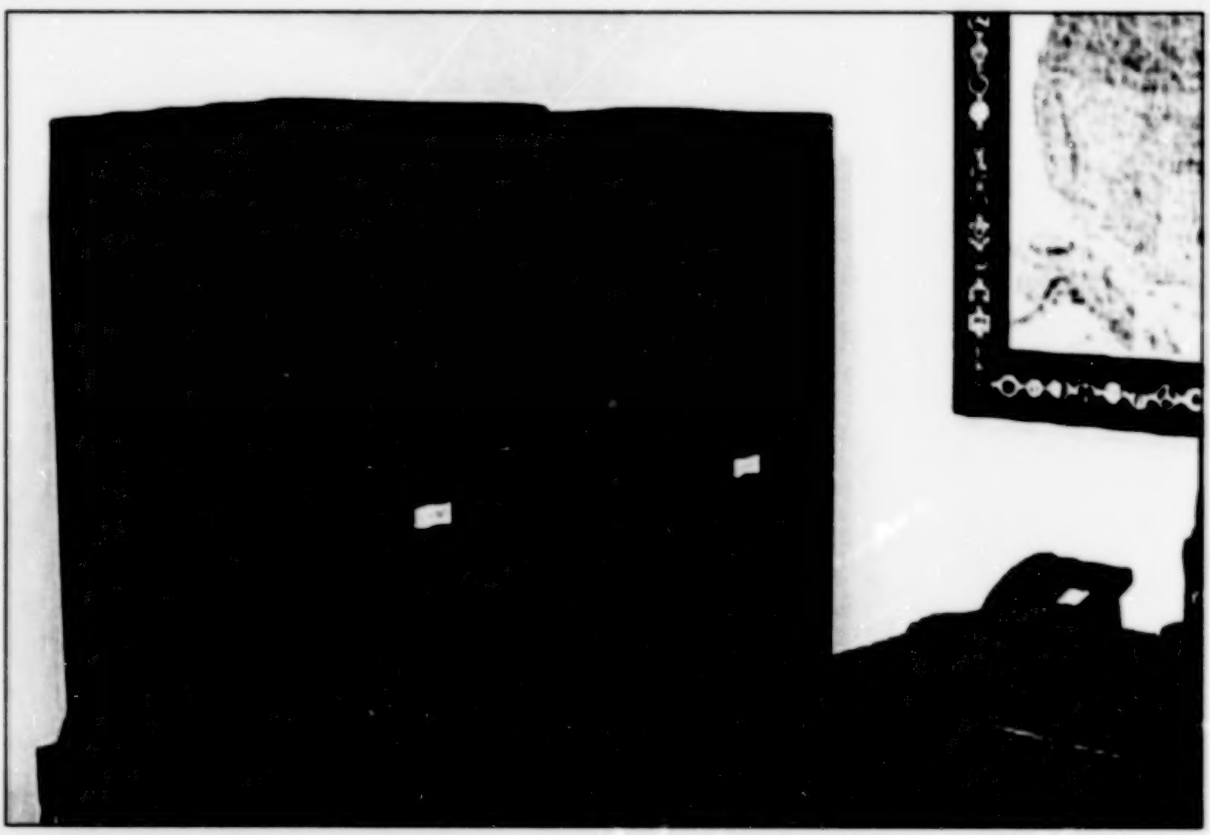
NATIONAL TELECOMMUNICATIONS COORDINATING NETWORK

The NTCN provides direct communications links between Federal departments and agencies and telecommunications carriers and equipment manufacturers during periods of widespread PN degradation or outages. This capability ensures timely dissemination of critical information to support network restoration coordination. Exhibit 3-4 provides a pictorial representation of the NTCN.

The NTCN relies on the NCC conference bridge to enhance the existing connectivity and capability. The conference bridge interconnects various types of communications systems, including HF radios, NCC dedicated ringdown circuits, communications satellites, the PN, and the National Telecommunications Alliance's Alerting and Coordination Network, thereby enabling conversations between users of these disparate systems. During FY 1999, the OMNCS implemented a number of changes to improve NTCN operation during the Y2K rollover. These changes are discussed in the preceding Y2K section.

Exhibit 3-4

Enhanced NTCN Components



TELECOMMUNICATIONS SERVICE PRIORITY PROGRAM

The FCC issued a report and order on November 17, 1988, establishing the TSP Program. The TSP Program is the regulatory, administrative, and operational framework for the priority provisioning and restoration of NS/EP telecommunications service. Under the rules of the TSP Program, service vendors are authorized and required to provision and restore services with TSP assignments before services without such assignments.

TSP OPERATIONS

During FY 1999, the Operations Division of the Office of Priority Telecommunications (OPT) received a weekly average of 255 requests for TSP restoration assignments. The OPT noted that State and local organizations constituted the largest growth area for TSP restoration assignments in FY 1999. This is attributable, in large part, to contingency planning of NS/EP organizations for the Y2K transition. In addition, priority provisioning of telecommunications services supported military operations in Kosovo.

The OPT, in conjunction with the TSP Oversight Committee (OC), analyzed the potential implications of LNP and evolving technologies, such as Internet services, on the TSP Program. With regard to LNP, the parties agreed that TSP users must ensure that telecommunications carriers are aware of circuits with TSP assignments that are supporting ported telephone numbers. With regard to evolving technology, the TSP OC formed a working group to facilitate ongoing analysis of the implementation of packet-switched networks, such as Internet protocol networks, and associated implications for TSP services.

TSP INFORMATION TECHNOLOGY SOLUTIONS

Throughout FY 1999, the OPT continued enhancing TSP Program information technology (IT) tools, including the TSP client-server. The OPT recognizes the importance of IT solutions to improve information flow and to expedite the process for requesting priority provisioning and restoration of telecommunications services for NS/EP users.

The OPT added a remote printing capability, new search queries, and more user-controlled administrative features to the client-server system. To further enhance their capabilities, the OPT updated its continuity of operations plan, including procedures to use a full backup client-server database at a remote location. The backup system will provide for continuity of TSP operations under any circumstance.

Also, the OPT enhanced the TSP World Wide Web home page to efficiently expand the information available to existing and potential TSP Program participants. Updates to text, improved navigation capabilities, and greater use of graphics increased the site's usefulness. In addition, the updated versions of the *Service User Manual for the TSP System* and the *Service Vendor Handbook for the TSP System* are available on the site in several formats for easy accessibility. The OPT also developed and implemented TSP Program electronic forms, which are available via a secure page on the Web site. These forms offer distant State and local TSP users and smaller telecommunications vendors an easy, secure, and universal mechanism to perform various required TSP processes.

TSP OUTREACH STRATEGY

The OPT modified its outreach strategy and associated outreach materials in FY 1999. The OPT recognized the importance of informing new telecommunications service providers, including competitive LECs and resellers, of their TSP obligations to ensure end-to-end priority treatment of facilities supporting NS/EP services. To assist with this effort, the OPT distributed a *TSP System Guide for Telecommunications Carriers*. The Guide outlined TSP vendor responsibilities to ensure that TSP Program priorities take precedence over other

telecommunications prioritization. To encourage expanded use of the TSP Program among critical infrastructures, the OPT targeted many gas and electric utilities for TSP training. The OPT developed a detailed TSP briefing to convey a thorough understanding of the TSP Program to these utilities. The briefing offered information on the legal background of TSP, TSP Program participants' responsibilities, and an overview of the TSP qualification and request process.

Educating and training emergency responders about the TSP Program remained a priority with the OPT. OMNCS personnel provided comprehensive training to potential Federal, State, and local users, vendors, and emergency response coordinators. It also provided training on the TSP client-server computer platform to agencies that frequently request TSP assignments. This resulted in a 27 percent increase in the number of users, including many from the private sector, involved with planning for Y2K contingencies.

NORTH ATLANTIC TREATY ORGANIZATION CIVIL COMMUNICATIONS PLANNING COMMITTEE

The OMNCS represents the United States on the NATO CCPC, its telecommunications working group, and other subsidiary bodies. The DOS detailee to the OMNCS is the Head of Delegation. CCPC purview extends to telecommunications and postal services. The OMNCS accordingly consults closely with U.S. commercial telecommunications service providers and affected U.S. Government agencies and organizations. The CCPC met twice in plenary session at NATO headquarters in Brussels, Belgium, during FY 1999; its telecommunications working group met four times and postal working group met one time.

In April 1999, three new member nations were brought into the NATO Alliance — Czech Republic, Hungary, and Poland. These nations are full participants in CCPC activities. In addition, 25 Partnership for Peace nations were invited to participate in the CCPC at the plenary level. It is anticipated that these 25 Partnership for Peace nations will eventually become participants at the working group level as well.

Some major CCPC FY 1999 activities and accomplishments included the following:

- Approved the committee's new work program for 1999–2000 based on NATO's new Strategic Concept and Ministerial Guidance. The work program includes civil emergency planning, crisis management, civil/military cooperation, and cooperation with Partner nations.

- Implemented a joint United States/United Kingdom effort to identify and test NATO authorized secure voice equipment.

- Completed a paper on network management, leading from peacetime to crisis.

- Completed a paper on the benefits and vulnerabilities of intelligent networks and their possible effect on NATO civil emergency planning.

- Began a thorough review of the CCPC, its taskings, and proceedings.

- Visited the three new NATO member nations to discuss mutual civil emergency planning concerns.

- Began preparations for CCPC participation in Crisis Management Exercise 2000.

The Alliance has once again identified the CCPC as a major committee in emergency planning under the new crisis management arrangements. A direct link between the CCPC and the NATO Command, Control, and Communications (NC3) Board has been created to allow the NC3 to provide direct tasking to the CCPC.

TELECOMMUNICATIONS ELECTRIC SERVICE PRIORITY

The U.S. Government telecommunications policy is to meet NS/EP requirements and supply adequate and secure electric energy to critical telecommunications facilities. In 1987, the Department of Energy, in coordination with the NCS and the NSTAC Energy Task Force, developed the Telecommunications Electric Service Priority (TESP) initiative.

The purpose of the TESP initiative was to enable essential national defense and civilian requirements to be met if an event, natural or manmade, disrupted electric supplies to critical telecommunications facilities. Before TESP, the electric utility priority restoration systems reflected only essential State and local needs. The TESP Program promotes modification of the existing electric utility emergency priority restoration systems to include telecommunications facilities considered critical to NS/EP. The critical link between electric utilities and telecommunications facilities provided by the program is an essential component to the response arsenal, particularly when damage to NS/EP assets may be national in scope.

Currently, 180 telecommunications service providers and 501 electric utilities support the TESP Program. As of April 1999, the total number of critical telecommunications facilities was 3,271.

SHARED RESOURCES HIGH FREQUENCY RADIO PROGRAM

The SHARES HF Radio Program continues to provide emergency communications in support of special operations and all-hazards situations. SHARES now incorporates the resources of more than 1,130 radio stations backed by 72 industry, Federal, and State organizations into a nationwide emergency message handling network.

The SHARES HF Interoperability Working Group, a permanent body established under the NCS Committee of Principals and Council of Representatives, published a revised SHARES directory on CD-ROM and revised the structure of the nationwide SHARES Coordination Network adding five regional stations. Those stations continue to conduct weekly check-in exercises. Since the check-ins began, the number of stations participating has increased from 20 to 140 stations per week. More than 5,000 check-ins were recorded in calendar year 1998.

The working group continues to conduct three nationwide readiness exercises each year. The overall exercise objectives are to:

- Provide personnel training on operating procedures and message formats
- Expand SHARES awareness within the Federal emergency response community
- Assess the interoperability of new HF technologies.

SHARES exercises were conducted in December 1998, involving 262 stations and 515 messages. The exercise provided the National Guard with information on the SHARES role in supporting the National Guard's Y2K Continuity of Operations Program (COOP). Additional exercises conducted in April 1999, supported the Department of Veterans Affairs and the Department of Health and Human Services emergency training objectives.

The SHARES Master Coordination Station KGD-34 continued to operate from the newly renovated NCC. The NCC Radio Operations Center is configured for voice, data, automatic link establishment, HF to telephone, and HF e-mail operations. The center also maintains two 24-hour HF bulletin board systems, and nine HF antennas.

COMMUNICATIONS RESOURCE INFORMATION SHARING

The Communications Resource Information Sharing (CRIS) initiative continues to support NS/EP requirements. It serves as an

information source that identifies communications assets, services, and capabilities for use by the participating NCS member organizations. Twenty-three industry and Federal organizations contribute more than 40 systems that could be shared with other Federal departments and agencies during emergencies.

As an emergency communications resource initiative, CRIS exists to support all-hazards situations. Potential users of CRIS coordinate requests directly with the OMNCS, thus ensuring their requests will not interfere with other ongoing activities.

TRAINING, EXERCISE, AND REGIONAL SUPPORT

The Operations Division TERS mission encompasses nationwide outreach through:

- Telecommunications Emergency Response Training (ERT) Seminars
- Internal and External Exercises
- Regional Planning Support
- OMNCS Augmentee Program.

With an emphasis on providing emergency telecommunications services to the disaster site, TERS achieves its program goal through a series of training and exercise activities and technology demonstrations. During FY 1999, TERS also focused on Y2K readiness programs, providing training and exercise support to various organizations. This support is detailed in the subsection entitled "Y2K Preparedness."

TRAINING

TERS is responsible for training OMNCS staff, NCS Regional Managers, Emergency Support Function-2 (ESF-2) support agency personnel, the telecommunications industry, and regional and State responders to effectively execute their responsibilities during the various phases of responses and recovery operations. During FY 1999, the TERS successfully coordinated and performed the following activities.

ERT Seminars. Because of the overwhelming success of the first two phases of the Telecommunications ERT seminars, TERS designed and developed ERT Phase III, which is scheduled to begin in February 2000.

EXERCISES

TERS conducts internal and external exercises to maintain expert knowledge of and proficiency in the management, integration, and employment of NS/EP telecommunications resources. In FY 1999, TERS successfully coordinated and performed the following exercises:

- ***COOP Orientation and Relocation Exercise.*** The COOP Orientation and Relocation Exercise provided industry representatives and EOT members with an overview of the COOP Plan and NCC Relocation Plan. The event was followed by a site visit to the relocation facility along with a tour of the NCS work area. A half-day training session preceded the exercise.

- ***Y2K Awareness Exercises.*** TERS supported FEMA in the development of a series of Y2K tabletop exercises. Please refer to the Y2K preparedness discussion for details of the exercises.

REGIONAL PLANNING SUPPORT

The OMNCS developed regional planning support to assist NCS Regional Managers across the 10 Federal regions. The goal of OMNCS support is to provide the NCS Regional Managers with capabilities, resources, and operational and functional support that will assist the Regional Managers in meeting ESF-2 mission requirements during activation and

41

nonactivation periods. OMNCS presence in the regions assists the Regional Managers in fulfilling their emergency planning duties. The OMNCS efforts include the following:

- Providing the NCS Regional Managers with operational planning documentation including procedures, program-specific checklists, and a coordinated national approach designed to standardize the best regional operational practices

- Realigning the OMNCS Augmentee Program to further support the needs of the NCS Regional Managers upon activation of ESF-2

- Supporting the NCS Regional Managers Conference that generated discussion on regional-level roles and responsibilities and emergency response planning and operations, and strengthened the NCS/GSA relationship at the national and regional level

- Supporting the NCS Regional Managers at various regional planning meetings, such as the RISC meetings

- Supporting FEMA and other national agencies at the Regional Y2K Workshops held in all 10 Federal regions

- Developing regional background information papers to assist the NCS Regional Managers and the OMNCS to better understand the regional environment

- Integrating new telecommunications technologies into regional planning efforts and establishing a role for the telecommunications industry in planning activities

- Continuing to develop disaster response after-action reports and ESF-2 lessons learned to capture regional best practices of the Federal Emergency Communications Coordinators supporting emergency telecommunications requirements of Federal, State, and local disaster response agencies.

TERS WEB SITE

TERS launched its inaugural Web site to provide emergency responders with the latest critical telecommunications and operational training, exercise, and regional support information. The site is divided into four main sections: overview, training, exercise, and regional support. The initial site is primarily informational but will feature additional interactive elements in the future. The current site includes such features as an online registration form for ERT seminars, a feedback option, a search engine, and other links of interest.

OMNCS AUGMENTEE PROGRAM

The OMNCS Augmentee Program continues to provide an important and valuable service to the NCS NS/EP mission at the national and regional levels. During Presidentially declared disasters, the Augmentee Program provides U.S. Army Reserve officers (skilled in communications) to support NCS and GSA Regional Managers during emergency operations and disaster response planning.

In the fall of 1998, the Augmentee Program was realigned to broaden OMNCS presence in the 10 Federal regions. This allowed the program to be more responsive to NCS Regional Managers when they are fulfilling their emergency planning duties. During annual training and drills, augmentees may now participate in a variety of planning and training opportunities for ESF-2 that support Regional Manager emergency telecommunications responsibilities.

INFORMATION SYSTEMS

The Operations Division Information Systems Branch implements and supports information systems required by the OMNCS at its primary and alternate sites. It provides technical support to OMNCS EOTs, offers help desk support to OMNCS staff, and coordinates OMNCS user IT requirements. The branch recently transitioned Emergency Response Link (ERLink) into full operational use.

EMERGENCY RESPONSE LINK

The ERLink Program is providing a controlled-access Web site designed to support communications within the emergency response community, including Federal, State, and local users. The ERLink Program office continued to focus on improving the response community's ability to share information. Exhibit 3-5 depicts the underlying network architecture of ERLink.

PLANS AND RESOURCES

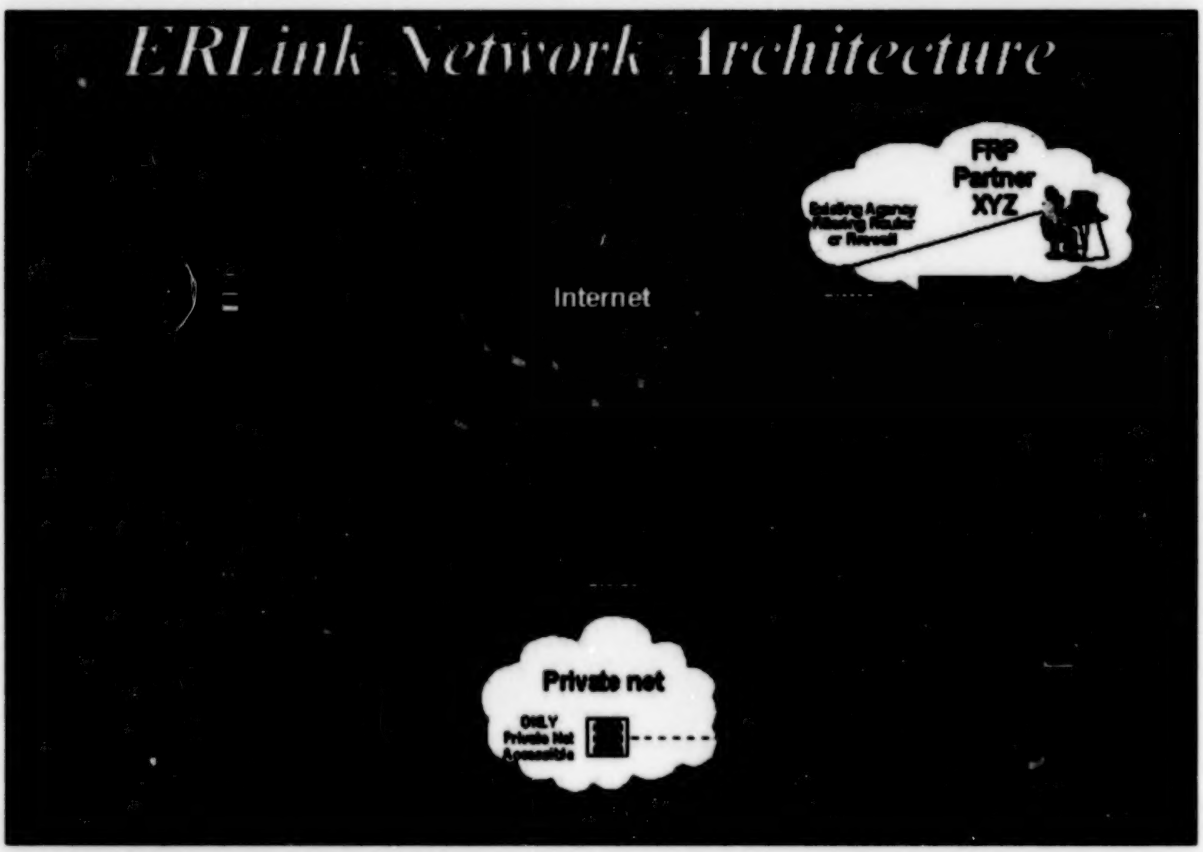
The Plans and Resources Division provides management and oversight for finance, acquisition, strategic planning, manpower, and all other resources supporting the OMNCS. The Plans and Resources Division activities include exercising authority and accountability over all resources allocated to NCS programs. The Division serves as the interface with the DISA directorates on financial and acquisition matters; DOD Planning, Programming, and Budgeting System (PPBS) documentation and execution; and acquisition management. The Division also conducts analyses and develops recommendations to the OMNCS and the DISA directorates on the optimal use of NCS resources to support mission requirements consistent with statutory and policy constraints.

PLANNING

The Planning Team documents leadership's near-, mid-, and long-term strategic direction,

Exhibit 3-5

ERLink Network Architecture



43

vision, and priorities through the development of the Strategic Plan, the Future Years Corporate Plan, and the Advanced Acquisition Plan. The Planning Team, through the implementation of the Performance Plan, comprehensively evaluates organizational performance and effectiveness.

FINANCIAL MANAGEMENT

For day-to-day operations, the Financial Team provides the overall fiscal direction for the OMNCS. The Financial Team develops and produces all PPBS-related documentation for the OMNCS, including program objective memorandums, budget estimates, the President's budget submissions, and all related exhibits. The team ensures that exhibits reflect decisions and directions from the Manager, NCS, and the DOD. The Financial Team also leads in the development, coordination, and implementation of funding procedures as directed and provides guidance and assistance to non-DOD agencies involved in the NCS to ensure that their requirements are met. Additionally, the team provides fund citations, ensuring the availability of funds and compliance with fiscal laws, regulations, and policies.

ACQUISITION MANAGEMENT

Acquisition support includes aiding OMNCS offices in all aspects of the Agency-level acquisition process. This includes preparing acquisition strategy documentation, statements of work, acquisition packages, proposal evaluation packages, and support documentation for NCS programs and projects. The Acquisition Team also monitors contractual performance and budget execution performance rates, identifies deficiencies, ensures reporting accuracy, and recommends adjustments.

CUSTOMER SERVICE

The Customer Service Division provides support to the NCS COP and COR and the President's NSTAC. Additionally, the division identifies and validates NS/EP telecommunications requirements to ensure NCS responsiveness to customer needs, develops threat assessments to NS/EP telecommunications and manages the Government and NSTAC Network Security Information Exchange (NSIE) process. The following paragraphs describe the Customer Service Division's FY 1999 activities.

NCS COMMITTEE OF PRINCIPALS/COUNCIL OF REPRESENTATIVES

The NCS COP and COR each met twice during FY 1999. These meetings focused on a number of Y2K-related topics as discussed in the "Y2K Preparedness" section. Additionally, the COP and COR concurred with the NCS response to the NSTAC XXI Executive Report, while the COP also voiced their approval of several NCS issuances discussed later in this section. The NCC Vision Implementation Team, composed of NCS agency representatives, continued its partnership with the NSTAC's Operations Support Group (OSG).

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

The President's NSTAC held its 22nd meeting on June 9, 1999, in Washington, DC. Major issues addressed at this meeting included the Y2K technology problem and critical infrastructure protection.

In keeping with its mission of providing the President with a unique source of national

security telecommunications policy expertise, the NSTAC approved several recommendations to the President. Among these were recommendations for the President to:

- Direct the establishment of a permanent program to address NS/EP issues related to the Internet
- Designate a focal point for examining NS/EP issues related to widespread adoption of electronic commerce within the Government
- Continue support for the efforts of the Department of Transportation to promote outreach and awareness within the transportation infrastructure, consistent with Presidential Decision Directive 63 (PDD-63)
- Direct the Federal Government to continue providing timely, meaningful, and accurate Y2K readiness and contingency planning information to State and local governments to enhance the flow of information to community Y2K groups and the general public.

NSTAC'S INDUSTRY EXECUTIVE SUBCOMMITTEE ACTIVITIES

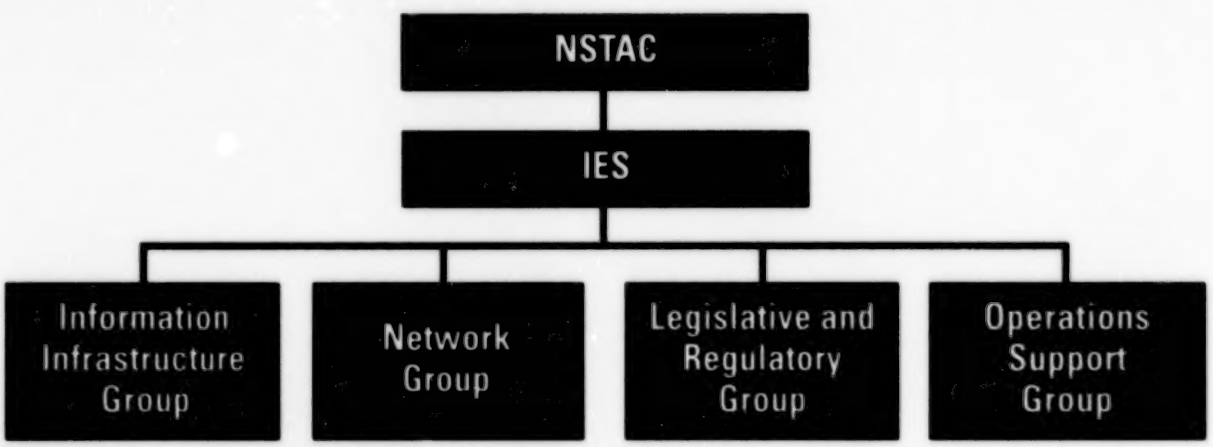
The NSTAC's IES continued to identify and develop issues for the NSTAC and direct the activities of its working groups. Infrastructure protection, network security, legislation and regulation, and industry/Government coordination and response were four key issue areas addressed by the IES and its working groups during FY 1999. Exhibit 3-6 depicts the corresponding organizational structure.

NSTAC'S INFORMATION INFRASTRUCTURE GROUP ACTIVITIES

In FY 1999, the Information Infrastructure Group (IIG) concentrated its efforts on several issues related to IA and infrastructure protection: transportation information infrastructure risks, global information infrastructure (GII), electronic commerce (EC), cyber crime, and PDD-63.

Exhibit 3-6

The President's National Security Telecommunications Advisory Committee Organization



45

Transportation Information Infrastructure Risk Assessment. In March 1999, the IIG hosted a second transportation workshop to provide a forum for representatives from all transportation sectors to discuss industry trends, including increased reliance on IT and the rapid growth of intermodal transportation. The workshop capped the group's efforts to gather information about the transportation sector's dependency on telecommunications and information infrastructures. The IIG used the findings from the workshop to complete the group's transportation information infrastructure risk assessment. Based on the risk assessment, the NSTAC recommended that the President continue to support the efforts of the Department of Transportation to promote outreach and awareness within the transportation infrastructure as expressed in PDD-63.

Global Information Infrastructure. In October 1998, the IES tasked the IIG to predict the characteristics of the GII in 2010 and to assess the implications for NS/EP communications. The group is researching and gathering information from industry and Government experts on NS/EP issues related to emerging space and land-based telecommunications systems. The group expects to complete the GII analysis in preparation for NSTAC XXIII.

Electronic Commerce. In FY 1999, the IIG continued its investigation of NS/EP implications associated with the adoption of EC in industry and Government. The subgroup focused its efforts on issues associated with the changing business and security processes and policies necessary to implement EC. In its final report, the IIG recommended that the President designate a focal point for examining the NS/EP issues related to widespread adoption of EC within the Government. The IIG also recommended that the President direct Federal departments and agencies, in cooperation with an established Federal focal point, to assess the effect of EC technologies on their NS/EP operations.

Cyber Crime. At the September 1998, NSTAC XXI Executive Session, the Attorney General requested that the NSTAC and the Department of Justice (DOJ) work together to address cyber security and crime. Through subsequent deliberations with DOJ officials, the IES determined that the NSTAC could help facilitate collaboration between the DOJ and the private sector. The result was a partnership between DOJ and the Information Technology Association of America (ITAA) and private sector companies —- labeled the "Cyber Citizen Program."

Presidential Decision Directive 63. IIG members continued to build relations with Federal officials responsible for PDD-63 implementation and shared lessons and successes of the NSTAC, offering NSTAC as a possible model for other infrastructures. The NSTAC will continue to partner with the Government and relevant private sector organizations as PDD-63 implementation proceeds.

NSTAC'S NETWORK GROUP ACTIVITIES

Issues related to network security R&D and the NS/EP implications of Internet technologies dominated the NG's work during FY 1999.

Research and Development. As a follow-on to the Intrusion Detection Subgroup's (IDSG) work, the NG sponsored an R&D Exchange to address the growing convergence of telecommunications and the Internet and how industry, Government, and academia should collaborate on network security R&D. The R&D Exchange occurred in October 1998, in cooperation with the OSTP, Purdue University, and the Institute of Electrical and Electronics Engineers.

The findings and recommendations of the participants in the R&D Exchange were documented in "Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration." As part of its follow-up on the R&D Exchange, the NG

noted that these findings and recommendations of the R&D Exchange were consistent with and validated those of the NG's IDSG Report issued in December 1997.

NS/EP Implications of Internet Technologies. The NG initiated its examination of the NS/EP implications of Internet technologies as a result of discussions on NSTAC's Widespread Outage report held at the December 1997, NSTAC XX meeting. During FY 1999, the NG completed its examination and prepared a report of its findings and recommendations for the June 1999, NSTAC XXII meeting. The report concluded that the NS/EP community's direct dependence on the public Internet for mission-critical operations is currently modest. Although departments and agencies use the public Internet, concerns about the Internet's reliability and security have caused them to limit their use to functions such as outreach, information sharing, and e-mail. For mission-critical NS/EP functions, the NS/EP community uses dedicated transmission control protocol/Internet protocol (TCP/IP) networks (also called intranets) because these networks give user organizations greater control of network elements. However, the interconnected nature of the public Internet means that a disruption or degradation of public Internet operations can nonetheless affect the availability, reliability, integrity, and user confidentiality of those dedicated TCP/IP networks.

The NG also concluded that NS/EP dependence on the public Internet is likely to grow steadily over the next several years, in part, because the public Internet offers a cost-effective and efficient means of communication, and industry and Government are moving toward a paperless, digital society.

These conclusions led to two recommendations to the President and further work for NSTAC:

- The first recommendation is for the President to direct the establishment of a permanent program to address NS/EP issues related to the Internet. The goals of such a program would be to increase understanding of evolving Internet dependencies and awareness of NS/EP requirements, and to investigate, develop, and employ NS/EP-specific priority services.

- The second recommendation is for the President to direct the appropriate Government departments and agencies to make use of existing industry/Government partnership mechanisms to increase awareness of NS/EP requirements within key Internet organizations and standards bodies.

NSTAC'S LEGISLATIVE AND REGULATORY GROUP ACTIVITIES

The Legislative and Regulatory Group (LRG) considers legislative, regulatory, and judicial actions that could affect NS/EP telecommunications. Following the September 1998 NSTAC XXI Executive Session, the LRG was tasked to identify and assess the legal and regulatory obstacles to sharing outage and intrusion information. To that end, the LRG determined that identification and discussion of existing and proposed NS/EP-related outage and intrusion information sharing channels could provide additional insights to assist the IES in assessing critical information sharing issues, particularly those associated with the implementation of PDD-63. To better understand the information sharing environment and the entities involved in the process, the LRG developed a report to illustrate the entities with whom telecommunications companies share outage and intrusion information, and to review the potential legal barriers that could inhibit the information sharing process.

During FY 1999, the NSTAC also tasked the LRG to identify possible barriers to the adoption of the wireless telecommunications priority access rules by the FCC and to evaluate NSTAC's level of continued support of the Cellular Priority Access Service (CPAS). Although

actions to establish CPAS are still under advisement by the FCC, the Commission has taken no final action. The LRG reported that, due to a number of factors, the OMNCS is addressing a new approach for providing wireless priority access based on channel reservation rather than on the technology originally proposed for CPAS.

NSTAC'S OPERATIONS SUPPORT GROUP ACTIVITIES

The OSG continued to evaluate the overall progress and direction of NS/EP telecommunications operational activities. In FY 1999, the OSG activities were focused on the NCC and Y2K.

NCC Vision-Operations Subgroup. The NCC Vision-Operations Subgroup continued to assess the mission, organization, and capabilities of the NCC, in light of ongoing changes in technology, industry composition, threats, and NS/EP requirements. Specifically in FY 1999, the NCC Vision-Operations Subgroup reviewed the NCC's proposed revisions to the electronic incident intrusion reporting criteria/process flows, which were designed to guide NCC participants in reporting anomalous network behavior. The subgroup also assessed current participation in the NCC to determine whether further additions would enable the NCC to better fulfill its electronic IAW function. Agreeing that broader participation could better enable the NCC to meet evolving NS/EP telecommunications requirements, the subgroup developed a list of companies and Government departments and agencies as possible candidates for participation in the NCC.

Y2K Subgroup. The Y2K Subgroup facilitated meetings between industry and Government, helping to ensure that all aspects of the Y2K technology problem pertaining to NS/EP telecommunications were being considered and that appropriate contingency plans were being developed. Throughout FY 1999, the Y2K Subgroup collaborated with the NCC in their development of contingency plans to prepare for Y2K and improve intercarrier coordination for recovery from potential widespread outages.

The subgroup also initiated discussions with industry and Government entities regarding the creation of an international early warning system for telecommunications outages attributable to Y2K. Investigating the Y2K outreach efforts of the Federal Government, the Y2K Subgroup considered the importance of disseminating timely and accurate Y2K information at State and local levels. Additionally, the subgroup discussed the need for increased industry and Government interaction with the public to dispel misconceptions regarding the threat Y2K poses to all infrastructures, including telecommunications. These efforts resulted in an NSTAC recommendation to the President that focused on the need to provide timely, meaningful, and accurate Y2K readiness and contingency planning information to State and local governments and to the general public.

INFORMATION ASSURANCE ACTIVITIES

The Customer Service Division's IA activities included assessment of the electronic intrusion threat to NS/EP telecommunications and management and support of the Government and NSTAC NSIEs.

ELECTRONIC THREAT TO NS/EP TELECOMMUNICATIONS

In March 1999, the OMNCS produced a report entitled The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document. This report examines the electronic intrusion threat to NS/EP telecommunications systems and interconnected information systems

and provides a baseline for vulnerability analyses, risk assessments, and countermeasure development.

The report concluded that electronic intrusion will remain an extremely serious threat to the PN, NS/EP telecommunications, and interconnected infrastructure systems for the foreseeable future. The report noted that the electronic intrusion threat to NS/EP telecommunications also affects other critical infrastructures, since the United States is increasingly reliant on complex, networked information infrastructures for its national and economic security and the welfare of its citizens. Economic, political, and social dependence on these systems extends from national-level activities to individual communities and their residents.

The report suggested that in order to meet the potential threat, industry and Government must work together to improve information security practices, intrusion detection capabilities, and network restoral and reconstitution.

NETWORK SECURITY INFORMATION EXCHANGE ACTIVITIES

The joint meetings of the NSTAC and Government NSIEs allow industry and Government representatives to exchange information in a trusted environment on threats to and vulnerabilities of the public network. The NSIEs also operate a limited-access World Wide Web server to enhance the capability of members to exchange sensitive information outside their NSIE meetings.

During FY 1999, the NSIEs produced two documents: *An After- Action Report on The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment and An Assessment of the Risk to the Security of the Public Network.* During FY 1998, the NSIEs had sponsored a workshop on the insider threat to information systems and developed two white papers to provide background material for the workshop. The workshop offered an overview of the emerging insider threat and suggested measures organizations could take to reduce their vulnerability to it. In FY 1999, the NSIEs developed an after-action report reflecting the insights that emerged from the workshop discussion.

The NSIEs also completed their 1999 PN risk assessment. The NSIEs concluded that the findings of their 1995 risk assessment are still valid today: old vulnerabilities are still being exploited, even though fixes are often available; vulnerabilities in many of the PN's diverse technologies remain unaddressed; and the highly interconnected nature of technologies and networks adds greater vulnerability. In addition, the NSIEs identified three major factors that have exacerbated the overall vulnerability of the PN over the past 3 years: the Telecommunications Act of 1996, changing business practices, and the Y2K technology problem. Although the NSIEs could not state how the risk has changed over the past 3 years, they determined that there is little evidence that the overall risk has diminished since 1995, and a number of factors to suggest that it is growing.

NCS INFORMATION ASSETS

In performing its management functions, the OMNCS coordinated and maintained NCS issuances, published the *NS/EP Telecom News* and the *FY 1998 National Communications System* report, and managed information resources.

NCS ISSUANCE SYSTEM

The NCS Issuance System is the authority regarding the internal organization, policy, procedures, practices, and management of the NCS. In FY 1999, the COP endorsed revised issuances of NCS Directive 3-1, *Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP);* and NCS Manual 3-1-1, *Telecommunications ServicePriority(TSP)*

System for National Security Emergency Preparedness (NSEP) Service User Manual; and NCS Handbook 3-1-2, *Service Vendor Handbook for the Telecommunications Service Priority (TSP) System*.

NS/EP TELECOM NEWS

NS/EP Telecom News, published quarterly by the OMNCS, provides an NS/EP impact assessment for the NCS and NS/EP telecommunications community and helps the NCS member organizations keep abreast of legislative, regulatory, judicial, technological, and policy developments.

NCS HOME PAGE

The NCS home page (http://www.ncs.gov) provides Internet clients and browsers a chance to learn about the NCS and NSTAC. The home page contains NCS and NSTAC history, information about NCS and NSTAC programs and activities, and online versions of NCS and NSTAC publications.

Among the publications posted onto the NCS home page during FY 1999 were the FY 1998 NCS Report, NCS 35th Anniversary documents, the NSTAC XXII Issue Review and the NSTAC XXII Reports. The home page holds current and back issues of the *NS/EP Telecom News* and fact sheets on various NCS programs.

REQUIREMENTS

The OMNCS Requirements staff is responsible for identifying, evaluating, and validating NS/EP communications requirements for the NCS. The Requirements staff works in conjunction with the OMNCS Requirements Forum, which consists of representatives from each of the OMNCS divisions. The forum provides an ongoing process for identifying and discussing NCS requirements and applying the maximum agency expertise and experience toward addressing identified customer needs. In addition, the forum serves to optimize OMNCS customer interface and participation in the requirements process. The following paragraphs describe the accomplishments of the Requirements staff during FY 1999.

REQUIREMENTS SHORTFALLS ASSESSMENT

In May 1999, the OMNCS, through the Requirements Forum, completed the *NCS Shortfalls Assessment Report*. The report assesses the ability of industry, OMNCS, and Federal departments and agencies to meet customer-identified NS/EP communications requirements and other functional requirements. Specific requirements referenced in the report were identified by customers in various studies, after-action reports, and other documents dating back to 1993. Consequently, this first iteration of the *NCS Shortfalls Assessment Report* represents a "baseline" for ongoing requirements assessment work.

Based on the assessment of requirements and capabilities, the report identifies shortfalls that may require OMNCS or other agency efforts to resolve. Shortfalls are grouped into four categories:

- Category I Shortfalls (New Capability) Customer requirements that are not fully satisfied and for which there are no formal Government or industry programs

- Category II Shortfalls (Enhanced Current Capability) Customer requirements that are being addressed under current programs, but require additional OMNCS resources to fully satisfy customer needs

- Category III Shortfalls (Funded Requirements) Customer requirements that are not fully satisfied but are being addressed by ongoing OMNCS activities; these requirements are adequately funded at present, given the current budgets of the respective OMNCS divisions

▶ Category IV Shortfalls (Out-of-Mission Scope) Customer requirements that are not satisfied, but have been determined to be outside the scope of the OMNCS mission.

The shortfalls assessment identified no Category I, 5 Category II, 10 Category III, and 3 Category IV shortfalls. In addition to the Category I through IV shortfalls, 19 NS/EP customer requirements, which have since been satisfied by industry or Government programs, were identified during a review of reference materials from the past 6 years.

REQUIREMENTS IDENTIFICATION EFFORT

In May 1999, the OMNCS initiated efforts to actively solicit NS/EP communications requirements from the NS/EP community. There were three primary objectives for this effort:

▶ Obtain input directly from NCS customers concerning their NS/EP telecommunications requirements

▶ Identify new and emerging requirements

▶ Validate past work on customer requirements

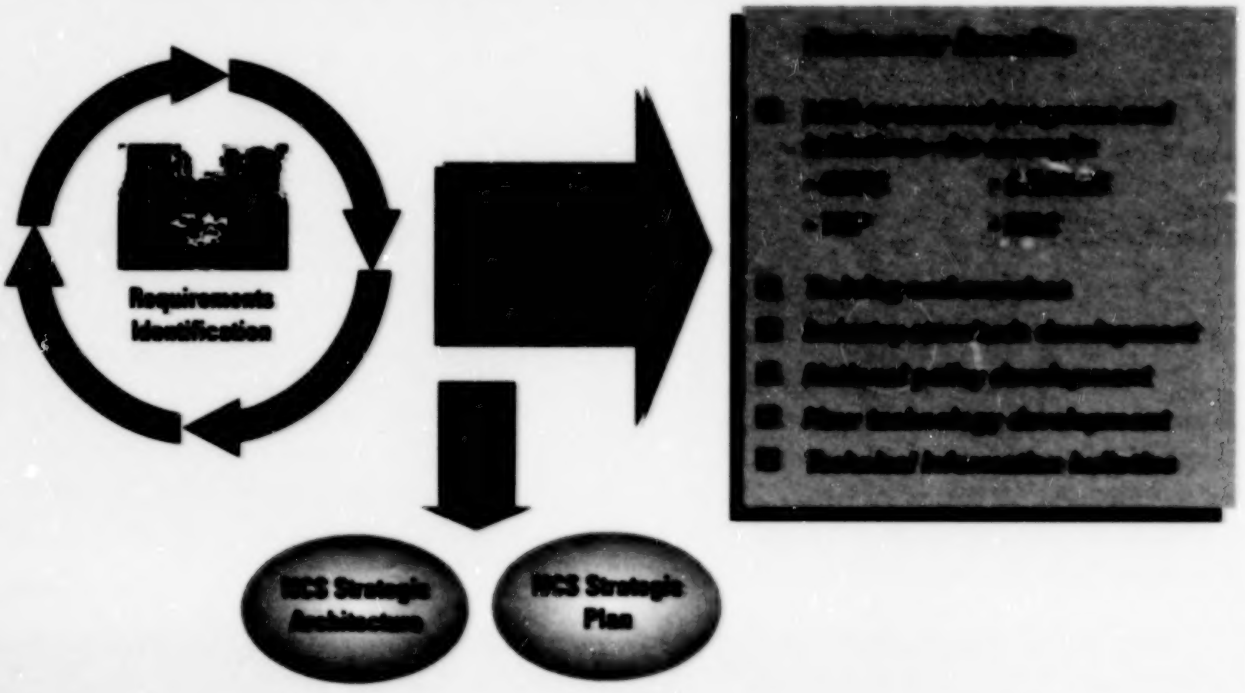
▶ Provide customers the opportunity to express their NS/EP needs for consideration in NCS program and initiative development

▶ Ensure more efficient and effective expenditure of limited NCS funds.

The emphasis of this effort was to identify requirements that would assist in developing programs and initiatives that would directly benefit NCS customers, while also supporting NCS strategic architecture and strategic plan development. See Exhibit 3-7 for requirements identification benefits.

Exhibit 3-7

Requirements Identification Benefits



STREAMLINING REQUIREMENTS TRACKING

While completing the *NCS Shortfalls Assessment Report* and collecting customer requirements, the OMNCS also worked to improve and streamline its ability to track NCS responsiveness to customer requirements. This effort resulted in the development of the NCS Requirements Tracking system. The database is designed to assist with requirements and shortfalls tracking, resource management, and report generation. It contains all information currently in the *NCS Shortfalls Assessment Report* and requirements identified since the report was completed. The database will be used to develop future shortfalls reports and will generate adhoc reports for NCS planning processes.

GAP ANALYSIS

The Requirements staff continued the efforts begun during the previous year to identify potential gaps between the Government's requirement for assured connectivity and what industry can provide. To test the process developed during the first pilot project with the Nuclear Regulatory Commission, the OMNCS initiated pilot projects with the Department of the Treasury (TREAS) and with the NCC.

Concurrently with the pilot efforts, and to facilitate timely, efficient, and consistent analysis of all OMNCS member agencies, the OMNCS initiated an effort to automate the gap analysis process. This effort involved incorporation of the following functions into an automated tool:

- Identification of the agency's NS/EP missions and functions
- Identification of minimum essential communications needed to sustain NS/EP activities
- Analysis of the agency's communications infrastructure supporting NS/EP activities
- Identification of any existing gaps between NS/EP communications requirements and the level of service available from industry.

The NCC study was still underway at the end of FY 1999. The TREAS study was postponed until development of the automated tool. Final development of the automated tool is expected during second quarter FY 2000.

IV

NS/EP TELECOMMUNICATIONS SUPPORT AND ACTIVITIES OF NCS MEMBER ORGANIZATIONS

DEPARTMENT OF STATE (DOS)

NS/EP TELECOMMUNICATIONS MISSION

The Department's mission is to support the President in formulating and executing U.S. foreign policy. This mission determines its telecommunications support requirements. Essential DOS telecommunications functions include:

- Implement and manage a reliable, secure, responsive, survivable, cost-effective, global telecommunications network.
- Provide communications support (including data, voice, imagery, facsimile, and video) for all U.S. Government agencies at U.S. overseas diplomatic facilities.
- Maintain a rapid response capability via alternative means to ensure the continuous availability of effective communications links under all conditions.

TELECOMMUNICATIONS STAFF ORGANIZATION

DOS manages its telecommunications through the Bureau of Information Resources Management (IRM) and the Diplomatic Telecommunications Service Program Office.

DOS SIGNIFICANT ACCOMPLISHMENTS

Modernization Efforts	The Department upgraded its mainframe systems in support of mission-critical systems modernization and Year 2000 (Y2K) activities. The Department also modernized five of the mission-critical mainframe applications and awaits Y2K certification. A Y2K-compliant platform is replacing the mainframe operating system software platform. Currently, 9 of 12 mainframe partitions are Y2K compliant and await Y2K certification. All mainframe related systems are on track to meet the Y2K compliance testing criteria. Having remedied all 59, or 100 percent, of its mission-critical systems, the Department also constructed new Y2K-compliant central infrastructures for both its unclassified and classified e-mail systems. The Department moved from an "F" to an "A" on the Y2K agency report cards issued by the House Subcommittee on Government, Management, Information and Technology. The three-tiered architecture principle serves as the basis of the design for both networks and uses the X.400 transmission protocol. Through the A Logical Modernization Approach program, the Department has completed the installation of Y2K-compliant infrastructure at 229 posts (98 percent) and established enterprise network management capability to maintain the global network infrastructure.
Primary Telegram Processing System	The Department replaced its primary Major Relay Station processor and Main State Messaging Center telegram processor with Concurrent 3280 systems.
Wireless (Radio)	The Department started an overseas wireless modernization program that will deploy state-of-the-art emergency and evacuation radio networks to 260 overseas posts as part of the Federal Government's efforts to enhance security at posts abroad.
Communications Security	The Department's Anti-Virus Program scanning for malicious code viruses "on the fly" was expanded to include File Transfer Protocol and Hypertext Transfer Protocol and the SIPRNet e-mail firewall gateways. Given the success of the InterScan VirusWall product, the real-time scanning of inbound and outbound Internet e-mail traffic program is being supplemented by installing Trend Micro ScanMail for Windows NT Exchange Server. This latter initiative will allow on the fly scanning of e-mail traffic and individual exchange mailboxes internal to the Department. Anti-Virus Web pages containing support material for the ScanMail product have been posted to the classified "ClassNet" and unclassified "OpenNet" Web locations. The IRM Y2K Committee approved the installation and distribution of the ScanMail software in CD-ROM format for general use statewide in August 1999. In addition, a new automated download utility for Norton Anti-Virus Software, Pre-Set Scanning Options, and Definition Update Files called Norton Systems Center (NSC) was received from the Symantec Corporation. Setup and installation support for NSC will be shipped to all bureaus and overseas posts in August. This product is not a replacement for the Norton Software Distribution Utility (NSDU) currently in use, but an updated version with enhanced diagnostic features not available in NSDU v2.0. The Department is continuing to develop its electronic Key Management System to strengthen its security posture for the protection of data transmissions. The Department's Certificate Authority Workstation is available for the production of Fortezza X.509 certificates at the sensitive-but-unclassified level. The Department established the Office of the Corporate Information Systems Security Officer responsible for ensuring the security regulation compliance of the corporate infrastructure and systems that connect to it.
Voice Program	The Department provided secure voice access to the domestic and foreign affairs community and assisted interdepartmental agencies in meeting their secure voice requirements.
Counter-Narcotics Program	The Department provided imagery, automated data processing, voice, and high-speed data services to the Department of Defense Counter-Narcotics Command Management System.
Support for the Secretary of State	The Department provided and supported protective radio packages for domestic and overseas protection of the Secretary and designated diplomats.

DEPARTMENT OF THE TREASURY (TREAS)

NS/EP TELECOMMUNICATIONS MISSION

The essential functions of the TREAS requiring NS/EP telecommunications are summarized as follows:

- Protecting the President, Vice President, their families, and other dignitaries
- Managing the economic activities of the United States, including all monetary, credit, and financial systems
- Administering the laws pertaining to customs, taxes, alcohol, tobacco, and firearms
- Serving as the principal economic advisor to the President
- Accomplishing international economic and monetary control as it pertains to the well-being of the Nation
- Manufacturing currency, coins, and stamps, and establishing methods of exchange

TELECOMMUNICATIONS STAFF ORGANIZATION

TREAS manages telecommunications through the Office of the Deputy Assistant Secretary for Information Systems and Chief Information Officer (CIO), under the Assistant Secretary of the Treasury for Management. Under this office, the Director, Corporate Systems Management (CSM), oversees NCS liaison and NS/EP support activities. The Director, CSM, also provides management guidance and financial oversight to improve the Department's use of telecommunications systems. CSM ensures, through the exercise of program management authority, that TREAS bureaus have access to a cost-effective, technologically sound telecommunications infrastructure that enables them to carry out their missions.

The TREAS CIO also serves as the Government Information Technology Service (GITS) Board vice chairperson. In this capacity, the TREAS CIO is responsible for developing information technology applications to improve Federal Government performance within the National Performance Review framework. The GITS Board affords significant opportunities to examine and enhance NS/EP, with emphasis on law enforcement and security initiatives and programs.

ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Gap analysis	TREAS is participating in the analysis of Government officials' expectations for telecommunications service compared with the capabilities offered by the public service communication providers. The outcome of that analysis is a definition of the gaps between what is expected and what can be provided.
Federal Law Enforcement User Group (FLEWUG)	TREAS has continued its activities as co-chair of the FLEWUG. This group is working to ensure that a cost-effective, interoperable, nationwide tactical wireless network will be developed for use by Federal, State, and local law enforcement and public safety groups.
Computer Emergency Response Capability	A formal computer emergency response capability working group was formed with representation from all the bureaus and departmental operations. The group's mission is to determine the best way to develop this emergency response capability for a variety of areas. Priority was placed on defining incident reporting standards and procedures. TREAS completed the year without being subjected to any publicly embarrassing compromises of its electronic data systems. The Department hopes to continue this trend while enhancing the intrusion prevention, detection, and remediation capabilities it now has in place.
Support for the Federal Public Key Infrastructure (PKI) Development	TREAS provided technical, budgetary, and leadership support for the development and use of an interoperable government-wide PKI to permit electronic transactions over the Internet in a trusted environment.
Counterfeit Checks Catalog	The Secret Service deployed a Web-enabled Counterfeit Checks Catalog that enables banks to register certain fraudulent activities (counterfeit corporate checks). This database allows near real-time access to information that previously took more than 90 days to be provided. This program, initially piloted in the Washington, DC–Baltimore area, has essentially controlled the local problem and has now been expanded nationwide.

DEPARTMENT OF DEFENSE (DOD)

NS/EP TELECOMMUNICATIONS MISSION

Under the provisions of E.O. 12472, DOD is assigned the following NS/EP telecommunications responsibilities:

- Provide, operate, and maintain the telecommunications services and facilities to support the National Command Authorities and execute the responsibilities assigned by E.O. 12333, United States Intelligence Activities, December 4, 1981
- Ensure that the Director, National Security Agency (NSA), provides the technical support necessary to develop and maintain adequate plans for the security and protection of NS/EP telecommunications
- Execute the functions listed in Section 3(l) of E.O. 12472.

TELECOMMUNICATIONS STAFF ORGANIZATION

DOD includes the Office of the Secretary of Defense, the military departments and the services within them, the unified commands, and other agencies established to meet specific U.S. military requirements. The Defense Information Systems Agency (DISA) is a separate DOD Agency under the direction, authority, and control of the Assistant Secretary of Defense (ASD) for Command, Control, Communications and Intelligence (C3I).

The principal staff positions concerned with NS/EP telecommunications in the OSD are the Under Secretary of Defense for Policy and the ASD for C3I. Command, Control, and Communication systems are the concern of a directorate of the Joint Staff.

DOD SIGNIFICANT ACCOMPLISHMENTS

Joint Task Force-Computer Network Defense	In December 1998, the Secretary of Defense created the Joint Task Force-Computer Network Defense (JTF-CND) after exercises and real-world events demonstrated the need for DOD to have a single coordinating organization to direct the defense of vital national computer networks. On Oct. 1, 1999, the U.S. Space Command assumed responsibility for the JTF-CND and brings the resources, advocacy, and warfighting authorities of a commander-in-chief (CINC) to the mission. The JTF is the department's focal point for defending DOD computer networks and systems in order to maintain its ability to plan, coordinate, and execute military operations. The JTF concentrates on computer network defense from an operational standpoint and exists to help ensure that warfighters can trust and rely on their computer networks and systems. The JTF becomes the DOD lead when computer network incidents cross CINC, Service, or Agency boundaries or could have a widespread effect on the Defense Information Infrastructure (DII). The JTF maintains a watch 24 hours a day, 7 days a week and has an assigned component force from each of the military services and DISA.
Year 2000 (Y2K) Issue	DOD has made tremendous progress toward fixing Y2K computer problems. DOD believes that they have identified and addressed the vast majority of systems requiring repair or replacement, especially those considered critical to the support of military operations. DOD fully expects to be capable of executing our part of the National Military Strategy on January 1, 2000, unimpeded by date-related failure of DOD systems.
Defense Information Network (DISN)	In fiscal year 1999, DISA, in coordination with the services and agencies, installed and commissioned unclassified and/or secret DMS equipment suites at about 85 major post/camp/stations, bringing the overall total to 230. This represents about 90 percent of the total number of sites required to make DMS the system of record for organizational messaging throughout the Department. DISA also fielded two major DMS releases, DMS 2.0 and 2.1. Both releases are Y2K compliant and passed an Operational Assessment (2.0) or an operational test (2.1). Testing included interoperability with the legacy AUTODIN system. Development of the next two releases also commenced.

DEPARTMENT OF JUSTICE (DOJ)

NS/EP TELECOMMUNICATIONS MISSION

The Department's mission is to provide telecommunications facilities and services in support of DOJ NS/EP essential functions. The Department centralizes its NS/EP responsibilities in the Justice Management Division for all Department entities except the Federal Bureau of Investigation (FBI). The bureau maintains separate secure network facilities.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Director, Telecommunications Services Staff (TSS) under the Deputy Assistant Attorney General for Information Resources Management, operates and manages DOJ's message processing systems and the Telecommunications Service Center. TSS also provides networking and technical assistance to DOJ's offices, boards, and divisions. Secure message transmission is offered through separate facilities (AUTODIN and Justice Automated Message System).

The Information Security Policy Group (ISPG), Security and Emergency Planning Staff is responsible for security oversight of all national security communications systems within the Department. The ISPG is the central office of record for all national security information key material for the Department. The Drug Enforcement Administration (DEA), FBI, and Immigration and Naturalization Services (INS) continue to administer their own communications security programs.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

DOJ continues to participate in the National Communications System (NCS) activities including the Committee of Principals and the Council of Representatives and other NS/EP telecommunications programs.

DOJ continues its vigorous support of NCS activities associated with the National Information Infrastructure, Government NS/EP telecommunications programs, NS/EP planning and contingency programs, and emerging NS/EP telecommunications programs.

DOJ actively participates in the Government Emergency Telecommunications System (GETS) Program, the Federal Telecommunications Standards Committee Standards Program, the Telecommunications Service Priority System Program, the Shared Resources High Frequency Radio Program, and the Communications Resource Information Sharing Initiative.

PENDING ISSUES

DOJ continues to monitor GETS for its impact on the Department.

DOJ COMMUNICATION SYSTEMS ASSETS/SERVICES:

- Automatic Data Processing Teleprocessing System
- DEA Nationwide Very High Frequency Radio System
- DEA Secure Voice System
- Global Criminal Justice Information System (Global)
- INS Tactical Radio System
- INS Integrated Network Communications
- Joint Automated Booking Station (JABS)
- Justice Consolidated Network (JCN).

DOJ SIGNIFICANT ACCOMPLISHMENTS

JABS	The Attorney General has established a JABS Program Management Office (PMO), responsibility for which has been assigned to the TSS. JABS is a DOJ initiative to develop a nationwide automated booking system. One of the primary goals of JABS is to streamline the identification and processing of Federal offenders throughout the criminal justice system. JABS will provide the means to electronically collect, store, and transmit photographic, fingerprint, and biographical data on offenders when they are booked. JABS is intended to minimize the processing time for booking an offender, eliminate redundant data collection, provide accurate information in a timely manner, and facilitate information sharing among Federal law enforcement components. Participants in the JABS project include the Bureau of Prisons, the DEA, the FBI, the INS, the United States Marshals Service (USMS), the Executive Office of United States Attorneys, and the Justice Management Division.
Global	Global has also been assigned to TSS. Global will fulfill a critical information sharing need of the entire criminal justice community. The Global concept was established by Vice President Gore in "Access America: Reengineering Through Information Technology." The Attorney General, who describes Global as DOJ's foremost information sharing initiative, has taken the leadership role in response to Initiative A07, Global. Under her leadership, DOJ is coordinating the achievement of a cost-effective global network capability in cooperation with local, State, and Federal criminal justice entities. Four actions were outlined in Initiative A07: (1) define the criminal justice community's information requirements; (2) test core requirements; (3) establish a joint Government-private sector Criminal Justice Information Network Advisory Group; and (4) prepare Global Criminal Justice Information Network plans. Global is defined as "the capability to communicate, exchange and retrieve timely, accurate, and complete information in an automated fashion with authorized elements of the justice community." This initiative recognizes that an information-sharing capability across the entire criminal justice community is essential for effective crime fighting. Fighting crime successfully requires the criminal justice community to share comprehensive case management, incident, investigative, and other data across local, regional, State, and national boundaries in real time.
	TSS's JCN, with Sprint as the service provider, continues to provide expanded operational telecommunications services by managing, engineering, and operating the DOJ nationwide data telecommunications systems serving all DOJ offices.

DEPARTMENT OF THE INTERIOR (DOI)

NS/EP TELECOMMUNICATIONS MISSION

The Department's mission is to efficiently manage the Nation's natural resources. DOI and the United States Department of Agriculture (USDA) co-manage the National Interagency Fire Center in Boise, Idaho. The center is the Nation's primary emergency support facility for forest fire suppression. From multiple radio caches strategically located throughout the United States, emergency mobile radio systems are available for fire fighting and other national emergencies. Forest fire suppression operations are conducted in close cooperation with State and local government emergency support activities.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Telecommunications Systems Division, Office of Information Resources Management, is responsible for DOI telecommunications program management. Bureau telecommunications managers and their staff are responsible for voice and data network operations.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

DOI implemented a nationwide communications network (DOINET) to support department-wide administrative applications, bureau programs, and other agency needs. The network's architecture is based on cell switching technology and consists of redundant switches and T1 circuitry for high reliability. Public asynchronous transfer mode network services have been added in response to increased bandwidth requirements resulting from Internet traffic being routed through the network to East and West Coast Internet exchanges.

The Alaska Regional Telecommunications Network, based on DOINET technologies, provides services to several Federal agencies in Alaska and uses DOINET to connect to the continental United States. These networks provide economical Internet and shared information processing system access. Shared use of these networks has lowered costs, improved performance, and increased the availability of data and video services. In addition, DOI and USDA are working together to improve operations by sharing telecommunications services, particularly where facilities are collocated.

DOI selected MCI WorldCom as its Federal Telecommunications System (FTS 2001) telecommunications supplier to replace AT&T/FTS 2000 services. Transition activities were initiated and switched voice services were moved to MCI WorldCom on a priority basis. The transition and redesign of the Department's data network services will commence in fiscal year 2000 with DOINET changing from a private network architecture to a virtual network on the MCI WorldCom public network.

DOI has a multivendor, multiyear contract to supply narrowband digital land mobile radios (LMR) and systems in response to the National Telecommunications and Information Administration mandated 10-year transition to narrowband LMR operations. This contract, available to all Federal agencies, makes lower cost, standardized, interoperable digital radios available throughout DOI and USDA. DOI is implementing a multiyear capital investment plan to ensure that all wideband very high frequency radio systems are replaced by narrowband systems before 2005.

Key officials, emergency coordinators, Year 2000 (Y2K) managers, and telecommunications specialists throughout the Department have Government Emergency Telecommunications Service (GETS) Cards for long distance emergency telephone communications. User policies and instructions accompanied distribution of GETS cards.

DOI SIGNIFICANT ACCOMPLISHMENTS

All DOI mission-critical systems have been certified as Y2K compliant and have undergone successful independent verification and validation testing. These systems include the DOINET and all bureau data subnetworks.

An Interior Site Information System was developed to provide a DOI Intranet-accessible inventory of telephone systems, data transmission equipment, circuits, facilities, and radio systems.

UNITED STATES DEPARTMENT OF AGRICULTURE (USDA)

NS/EP TELECOMMUNICATIONS MISSION

USDA has several essential functions requiring NS/EP telecommunications. These functions include domestically distributing seed, livestock, poultry feed, fertilizer, and farm equipment; managing the use of land and facilities under USDA jurisdiction; directing the rural fire control activities in national forests through coordination with local authorities; and, inspecting livestock, poultry, and other products to ensure the quality and safety of food.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

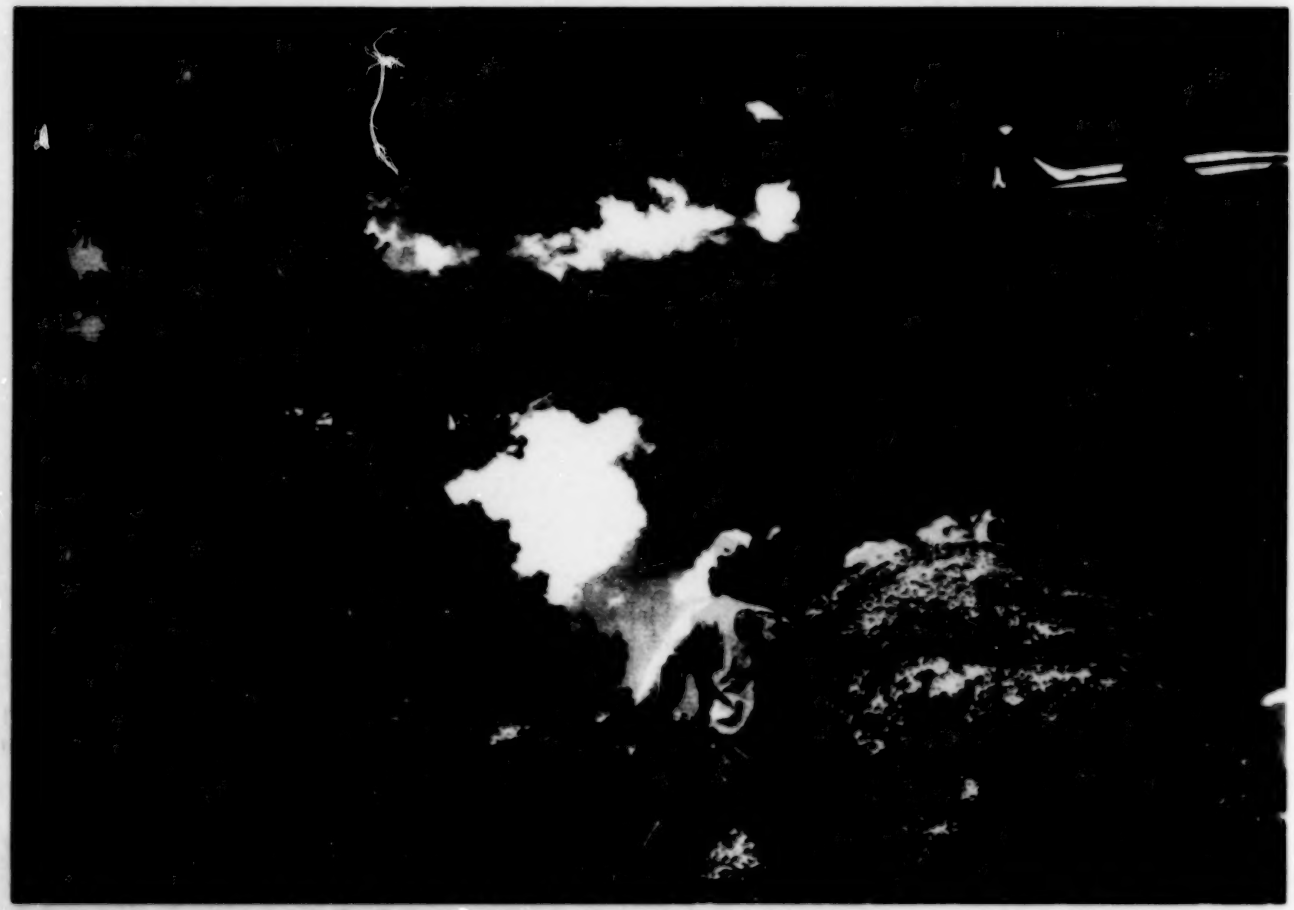
USDA continues to support the Government Emergency Telecommunications Service (GETS) program by working to increase the number of personal identification number cards provided to key NS/EP personnel within the Department. USDA has been expanding the GETS program within the Department to include key Year 2000 staff.

USDA also:

- Continues support for the Committee of Principals/Council of Representatives and the President's National Security Telecommunications Advisory Committee
- Participates on Shared Resources High Frequency Radio Program, Communications Resource Information Sharing Initiative, Federal Telecommunications Standards Committee, and Federal Wireless Users' Forum
- Supports the Department of State Diplomatic Telecommunications Service
- Participates in and represents the USDA on Cellular Priority Access Service, Federal Law Enforcement Wireless Users Group, and other working groups as necessary
- Maintains Secure Telephone Unit-IIIs throughout the Department supporting NS/EP functions.

NS/EP PARTNERSHIP ACTIVITIES

The Forest Service is currently conducting pilot tests of mixed analog/digital narrowband radio systems with the Department of Interior (DOI) Bureau of Land Management and is implementing several shared-agency systems. Animal and Plant Health Inspection Service has also entered into several shared-system agreements with DOI bureaus.



Reliable communications from firefighters to airtanker's keep wildfires contained.

DEPARTMENT OF COMMERCE (DOC)

NS/EP TELECOMMUNICATIONS MISSION

The DOC mission includes support for domestic and international trade; commodities, invention, economic analysis of census and industry, and technology related patents and standards. The Departmental technology role includes providing tools for monitoring and analyzing environmental weather, oceanic, and geophysical data for reporting of critical early warnings of emergencies to prevent loss of human lives and damage to property. These missions are ongoing and enduring to support national level NS/EP activities in all-hazard emergencies, including stress periods during peacetime, crisis and mobilization, as well as late trans-attack and early post-attack (LTA/EPA).

DOC missions are critical to the economic strength of the national infrastructure. They include 15 activities supporting NS/EP functions from Executive Orders 12656 and 12472 that require implementing plans during peacetime and activating plans during crisis/mobilization and LTA/EPA. The Federal Response Plan identifies DOC as a major supporter of six emergency support functions for national reconstitution and support to State and local identified critical functions. DOC has a major role in national level critical infrastructure protection (CIP) program supporting the communications and information segments, as well as a primary role in managing the center for CIP coordination (circa Fiscal Year 1999) as specified in Presidential Decision Directive 63. More information on these programs is available at the DOC web page, www.doc.gov .

CURRENT NS/EP TELECOMMUNICATIONS ACTIVITIES

- The International Trade Administration continues to upgrade data communication platforms supporting access to trade information at world trade centers and U.S. embassies overseas. This capability is linked to the Department of State Diplomatic Telecommunications Service network upgrades to support international communications between DOC trade offices.
- The National Oceanic and Atmospheric Administration (NOAA) and the National Weather Service (NWS) continue to implement the new telecommunication network supporting weather data collection and distribution platforms from field observation offices and processing centers.
- The Office of Administration (ADM) of the DOC is upgrading Continuity of Operations plans and support for critical missions and programs, and the DOC ability to continue operations at remote locations using contingency communications services.
- DOC/ADM continues to coordinate the Departmental use of Defense Information Systems Agency communications services from AUTODIN to Defense Message System. This service is used to communicate NOAA/NWS emergency weather information and alerts, such as tsunami and hurricane, and to collect weather observation data.
- DOC/ADM is implementing services department-wide from the new Federal Telecommunications System 2001 networking contract for contingency communications and special features supporting NS/EP (i.e., Government Emergency Telecommunications System [GETS], Telecommunications Services Priority [TSP]).
- DOC/ADM is conducting information technology (IT) assessments of its telecommunications support and networking to determine compliance with Government-wide Y2K requirements.
- NOAA/NWS continues to review and enhance its use of the shared resources (SHARES) program to support emergency communications capabilities in the field for severe weather observations and reporting.

PENDING ISSUES

To enhance NS/EP services, DOC uses all NCS support service programs, i.e., the National Coordinating Center for Telecommunications, TSP, GETS, SHARES, Communications Resource Information Sharing initiative, and Emergency Response Link for contingency communications. DOC serves as the lead Government agency implementing alternative communications technology with an interest in Cellular Priority Access Service. DOC operating units are continuing to expand their use of these services as more regions and locations acquire access. Funding and human resource factors continue to be key drivers for agency participation. Early program involvement by the agency is essential to agency use of NS/EP resources Government-wide.

DOC SIGNIFICANT ACCOMPLISHMENTS

NOAA/NWS new weather monitoring and reporting capability was commissioned in 1999 to provide communications services for the advanced weather information processing system.

DOC/ADM completed enhancements for administrative information systems to function with the Internet and Departmental intranet access using web browser technology to create accesses to publicly available information.

DOC SIGNIFICANT ACCOMPLISHMENTS (continued)

NOAA/OA expanded its use of frame relay network services to their domestic network and the network control centers to allow responsive support and alarm monitoring; the new Internet Protocol (IP) communications capability allows more robust communications with the five operating units for the transfer of information between major data centers.

NOAA/NWS installed additional Doppler radar systems as an effective weather information gathering platform and within the wind profiler program.

NOAA/NWS installed additional IP service products to enhance the communications of weather information between computing centers and regional customers using the Internet web.

NOAA/National Environmental Satellite Data and Information Service (NESDIS) enhanced its search and rescue satellite data network to collect and report emergency warning messages; this capability collects Global Positioning System data to further pin-point the source of emergency alarm signals, from distressed ships, planes, or terrestrial vehicles.

NOAA/NESDIS fully commissioned into operation the three-axis positioning geostationary operational environmental weather satellites (GOES) for gathering imagery information used in weather warnings and forecasts; the new capability collects earth images from two platforms - one in the eastern U.S.-Atlantic area and the second in the western U.S.-Pacific area (GOES East and GOES West, respectively).

NOAA/NESDIS initiated management and operational support of the Department of Defense Meteorological Satellite program under an agreement which will use the resources at DOC to centralize the operational support of the all weather satellites.

The Economics and Statistics Administration/Census Bureau upgraded its domestic network to meet year Census 2000 communications requirements between data collection and processing platforms; this capability supports the decennial census as well as the economic, labor and industrial census components of the economic infrastructure.

DEPARTMENT OF HEALTH AND HUMAN SERVICES (DHHS)

DHHS CURRENT/ONGOING ACTIVITIES

During numerous FY 1999 deployments, DHHS was grateful to the National Communications System (NCS) for the ability to utilize shared resources (SHARES) stations in the affected areas to aid in coordinating telecommunications resources. DHHS is also thankful for the Communications Resources Information Sharing (CRIS) initiative that NCS has continued to support.

DHHS continues to utilize and expand its ultra high frequency modulation radio assets. Other agencies have graciously made frequencies available for National Disaster Medical System (NDMS) use.

DHHS SIGNIFICANT ACCOMPLISHMENTS

DHHS increased the number of portable repeaters to better support disasters affecting a wide area or multiple simultaneous disasters. Repeater access tones are programmed so they can support Federal Emergency Management Agency Urban Search and Rescue Teams, which share a repeater frequency pair with NDMS.

NDMS is indebted to amateur radio operators for their assistance in disaster communications. Many of the Disaster Medical Assistance Team communications officers and communications specialists acquired the essential skills of disaster communications from their amateur radio experience. During hurricane deployments, the "Hurricane Watch Net" provides invaluable information about hurricane conditions and damage.

DEPARTMENT OF TRANSPORTATION (DOT)

NS/EP TELECOMMUNICATIONS MISSION

DOT comprises 10 Operating Administrations (OA) in partnership with transportation owners and operators that collectively make up the national transportation system with an economic impact of 11 percent of the gross domestic product. The OAs are guided by a Departmental Strategic Plan judged by Congress to be the best in the Government. The National Security goal is one of the five strategic goals outlined in the plan. DOT's NS/EP Telecommunications activities are aligned with this goal. Additionally, OAs have been drawn together by the OneDOT philosophy, which leverages the efforts of all OAs to better accomplish our mission. The Department demonstrates its commitment to enhanced NS/EP telecommunications through participation in the National Communications System (NCS) Committee of Principals and the Council of Representatives and through active participation in the President's National Security Telecommunications Advisory Committee and NCS initiatives related to Information Assurance, Critical Infrastructure Protection, and the Communications Functional Group for the National Emergency Management Team. DOT is a member of the National Coordinating Center for Telecommunications (NCC), Indications, Assessment and Warning pilot program. The Deputy Secretary has established a Year 2000 (Y2K) Outreach Assessment Team that partners with industry, the public, and the international community to ensure readiness of transportation systems and appropriate contingency and continuity plans.

ONGOING NS/EP ACTIVITIES

A prime example of the OneDOT concept is the Caribbean Emergency Communications Network. This is a network of seven high frequency (HF) radio stations and satellite terminals located in Puerto Rico; the Virgin Islands; Atlanta, GA; and Washington, DC with a mission of providing emergency communications support to the Southeast United States, primarily for disaster response and recovery. The Federal Aviation Administration (FAA) is the lead agency for this initiative and is in partnership with the U.S. Coast Guard (USCG), the Federal Highway Administration (FHWA), and the Office of Emergency Transportation (OET) of the Research and Special Programs Administration (RSPA). Monthly tests of this system ensure its continual readiness.

Two FHWA damage assessment teams traveled to Puerto Rico and the Virgin Islands in response to Hurricane Georges. The teams used three portable satellite terminals to set up an emergency operations center immediately upon arrival. During the same period, the USCG deployed two Transportable Communications Centers (TCC) to Puerto Rico to assist in search and rescue communications and restoration of the island's communications infrastructure.

USCG TCCs were also deployed to other diverse missions, such as oil spill contingency support, floods, counter drug operations in Haiti, and Y2K readiness exercises in Juneau, Alaska, and Washington, DC.

FAA, FHWA, and USCG stations actively participated in several Shared Resources HF radio exercises. Additionally, these agencies exercise connectivity with Federal Emergency Management Agency (FEMA) and the NCS National Telecommunications Coordinating Network. An HF radio exercise that FHWA conducted with the northeast region emergency representative included seven Coast Guard cutters and 13 shore units, all using emergency power. The USCG has conducted extensive contingency HF and satellite communications testing in preparation for Y2K.

The Maritime Administration (MARAD) conducted exercises with the U.S. Navy's Pacific Fleet. Exercises BELL BUOY 98 and JFTEX 99-1 tested communications interoperability among the Navy, MARAD, and more than 20 U.S.-flag merchant ships in the Persian Gulf and the Pacific.

DOT SIGNIFICANT ACCOMPLISHMENTS

The RSPA's OET hosted a Y2K exercise for the President's Year 2000 Council Information Coordination Center (ICC). In addition to all DOT agencies being represented in the DOT Crisis Management Center, the ICC staff also used the facility as their command center to test information-reporting procedures with key departments and agencies over the Julian day 99 of 1999 rollover.

FHWA has completed deployment of satellite telephones to 52 field offices. Although HF Radio remains a critical component of its central U.S. communications, FHWA has designated satellite as the primary communications method and conducts monthly exercises. FHWA's southern region will receive communications training during FY 1999 and the remaining 25 percent of offices will receive training in FY 2000.

The USCG Auxiliary has joined with FHWA and the Office of Emergency Transportation to permit volunteer USCG Auxiliarists to serve as backup operators of communications equipment in the DOT Crisis Management Center (CMC) during emergencies. This agreement also allows auxiliary radio stations to relay emergency messages nationwide to and from the CMC.

FAA has completed fielding of alternative satellite telephone systems for operational facilities. A communications van has been acquired for use by FAA's communications Support Teams responding to aviation incidents or supporting agency command and control requirements.

FAA saved $1.3 million by converting its dedicated circuit AUTODIN connections to a dialup service that is on the migration path to the Defense Message System.

DEPARTMENT OF ENERGY (DOE)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The Headquarters Emergency Communications Network (ECN) currently has 21 data and 18 video nodes, with planned expansion for up to 50 nodes, to DOE Emergency Operation Centers (EOC), Field Intelligence Units, and other Government agencies throughout the United States. The ECN is backed up by the Emergency Satellite Communications System and INMARSAT. Under the Material Protection, Control and Accounting Agreement between the Department of Defense (DOD) and the Ministry of the Russian Federation for Atomic Energy (Minatom), Headquarters will provide an unclassified communications link between the Minatom Situation and Crisis Center in Moscow, Russia, and DOE's EOC in the Forrestal Building, Washington, DC. The Headquarters Office of Emergency Management partnered with the Defense Intelligence Agency, the Air Force 497th Intelligence Group, and DOE's Office of Intelligence to implement the DOD Intelligence Information System AUTODIN Bypass System project. The project plans for the closure of the AUTODIN network and for DOE's Communications Support Processor to interface with the Joint Worldwide Intelligence Communications System in support of the Intelligence Community Defense Management System.

DOE plans to partner with a nationwide commercial vendor to develop a paging system for the Nevada Test Site and surrounding rural areas comprised of a single, two-way pager with national coverage capability.

Southwestern Power Administration's (Southwestern) Optical Ground Wire (OPGW) replaces faulty wire causing transmission line outages. The OPGW will interconnect Southwestern substations and offices operating the electric power system. Five hundred twenty-six miles of OPGW were installed throughout Arkansas and Missouri, allowing Southwestern to complete a digital communication path from its control center in Springfield, Missouri, to its maintenance office in Jonesboro, Arkansas. Southwestern plans to install 141 miles of OPGW in fiscal year (FY) 2000 and 98 miles in FY 2001 to replace aging power line carrier and analog microwave communication equipment.

Western Area Power Administration is replacing its existing conventional analog wideband very high frequency (VHF) mobile radio system with a new Motorola trunked-capable narrowband analog/digital VHF mobile radio system. The mobile radio system controls the operation and maintenance activity of the power transmission system. The existing 15-State system consisting of five distinct radio systems will be replaced with one homogeneous system.

Oak Ridge Operations Office is implementing Public Key Infrastructure to enable support of encrypted data network traffic.

DOE SIGNIFICANT ACCOMPLISHMENTS

In May, DOE's scientists, engineers, and program/project managers displayed two weapons incorporating counter-terrorist technologies focused on limiting terrorist acquisition of weapons of mass destruction. These weapons were on display at the Russell State Building for both Congress and the general public to view. The centerpiece of the Exposition was the ECN interactive video wall depicting departmental sites and employees in action.

During FY 1999, Headquarters implemented redundant, alternate OC-3, 155 mbps data network pathways to optimize transmission reliability, availability, and bandwidth-intensive applications between its Germantown and Forrestal facilities. DOE also implemented wired and wireless remote access services to enhance security and provide a common mechanism for data communication and access by remote customers. Finally, Headquarters upgraded its Northern Telecom SL-100 telephone system switch operating systems from BCS-36 to MSDL-07 versions for Year 2000 (Y2K) compliance.

Idaho National Engineering and Environmental Laboratory (INEEL) installed protected power systems to its primary paging system's transmission facilities. The paging system is the primary means of recalling EOC staff in an emergency. INEEL completed several projects within its data telecommunications network providing users with operational improvements and upgraded security. It completed the upgrade of its Nortel SL-1 NT Private Branch Exchanges (PBX) processors to Meridian Option 61-C. This upgrade increased the call processing capabilities for INEEL's telephone community serviced by 13 distributed PBXs, all of which are Y2K compliant. INEEL also completed an upgrade to the telecommunications network monitoring and centralized management system.

The Nevada Operations Office (NV) upgraded its Northern Telecom SL-100 telephone switch operating system from BCS-36 to MSL-08 and completed the conversion to OCTEL 350 voice messaging system. In conjunction with Federal, State, county, and city governments, NV successfully demonstrated emergency communications capability throughout the complex, during the "Sunrise 99" exercise.

The Hanford Site Fire Department's central dispatch center communications console was replaced to perform standard functions in the local community. Hanford also integrated the existing telephone and radio systems into one consolidated communications system. The Hanford Fire Department acquired a remote command center vehicle capable of setting up an on-scene command center for site emergencies. Finally, the Hanford radio paging system was upgraded using additional repeater stations to increase in-building radio pager coverage for that site.

The Oak Ridge Operations Office cut over a new telecommunications system composed of a main node with four remote switching modules. Each node is connected by a SONET-based, self-healing fiber ring and can function independently of the others with minor functionality loss. Each node also has critical bypass trunks for diverse routing and secondary dial tone.

Savannah River Operations Office (SR) completed the installation and connection of a classified audio, video and data communications system to the DOE Emergency Network in the Savannah River Site Operations Center. SR has transitioned its security and emergency response organizations to a new radio trunking system. In addition to meeting National Telecommunications and Information Administration mandates for spectrum efficiency, the new system provides better communications coverage, reliability, and security.

DEPARTMENT OF VETERANS AFFAIRS (VA)

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

VA WIDE AREA NETWORKING

VA embarked on a two-phase transition of the wide area network. Phase one, the migration of the physical (IDCU) network to the Federal Telecommunications System 2001 (FTS 2001) contract, was completed on June 1. Phase two of the transition involves the cutover to the Sprint PSN2 network. During the implementation of phase two, the Veteran's Health Administration (VHA) will implement a new wide area network paradigm. The Veteran's Integrated Service Network (VISN) is establishing multiple VISN networks that are subsequently connected to the national VHA ATM backbone. One expected outcome of this concept is that in the event of loss of connectivity to the national backbone, the VISN could remain operational and provide connectivity between facilities between multiple VISNs. VA cutover to the PSN2 network is expected to begin in October when the VHA ATM backbone is in place.

FTS 2001 TRANSITION

The current FTS 2000 contract expired December 7, 1998. However, it was extended for 1 full year with two additional 6-month options. The General Services Administration (GSA) awarded Sprint the first of two possible awards under the FTS 2001 contract with the second round, consisting of competitive pricing, awarded to MCI WorldCom. The two vendors will split a total minimum revenue guarantee of $1.5 billion. VA has selected Sprint to meet VA's essential telecommunications requirements. The FTS 2001 contract is expected to usher in a new era for Federal telecommunications procurement. Services will be more competitive, with better prices, greater flexibility, and provide more choices, as well as offer easier ways to acquire new technologies. Also, to assist in this "new era," VHA has a newly appointed VHA Delegated Agency Representative where the Communications Services Office (CSO) is staffing this function to ensure the promptest customer service possible.

YEAR 2000 (Y2K) COMPLIANCE ACTIVITIES

CSO (194D) started its work on Y2K issues related to VA medical centers' telephone systems in early March 1997. At that time, the VA service partnered with the GSA and Mitretek Corporation. Mitretek was contracted by GSA to help resolve all Y2K issues related to telecommunications equipment utilized by Federal agencies. CSO has completed Y2K compliance testing of all related major telephone system manufacturers and has distributed test results to the respective VA medical centers. Two hundred and forty sites reported Y2K status of their telephone systems, 21 sites reported noncompliance. CSO is actively working with the latter sites to ensure that these facilities will have telephone service in the year 2000 and beyond. These actions consist of supplying these facilities with information from the manufacturers about "patches" or other "work-around" alternatives, such as manual reset of equipment, that will be required to ensure minimal disruption, if any, to the medical center telephone systems.

As an additional contingency to other Y2K compliance endeavors, VA has identified "critical" locations to ensure not only that on-site telecommunications equipment is Y2K compliant, but that the local exchange carriers (LEC) providing network interfaces to these facilities are also compliant. In cases where the LEC is determined to be noncompliant, special arrangements were made to ensure network access.

GOVERNMENT EMERGENCY TELECOMMUNICATIONS SERVICE (GETS)

In anticipation of a crisis resulting from unforeseen Y2K issues, hundreds of "key personnel" within VA have been issued GETS cards. These cards, issued and managed by NCS, are to be used when normal or other telecommunications means prove ineffective in completing emergency calls.

VA NATIONWIDE TELECONFERENCING SYSTEM (VANTS)

VANTS provides all VA facilities with accessibility to 576 audio ports for voice teleconferencing. This service provides a means for VA employees, emergency personnel, state officials, and equipment vendors to communicate without losing time and incurring costs related to travel. Participants are provided a toll-free number for easy access from any telephone.

VANTS also provides a video bridge for videoconferencing over Integrated Services Digital Network (ISDN) and has ports on FTS Networks A and B, as well as commercial Bell Atlantic. This technology allows the staff to conduct videoconferences, such as business meetings, distance learning sessions, and interviews, including non-VA facilities, such as educational institutions, military installations, and vendors, without leaving the workplace.

VANTS audio and video teleconferencing services are available 7 days a week, 24 hours a day.

VA AMATEUR RADIO SERVICE

VA medical centers are authorized to establish and use on-campus amateur radio stations for therapeutic purposes in veterans health care programs. These amateur radio facilities fill a secondary role, that is, providing hospitals and local communities with reliable communications under emergency conditions. The VA Radio Frequency Management Office supports this activity with weekly releases of local and national Amateur News. VA amateur radio operators participate in local, regional, and national emergency exercises to enhance and maintain their operational capabilities.

OFFSHORE SATELLITE SERVICE

The Office of Telecommunications coordinates offshore Satellite Telephone Service via the International Maritime Satellite Organization (INMARSAT) to provide emergency voice and data telecommunications service to VA facilities operating in United States Territories and Possessions. Multiple portable terminal platforms are provided to ensure survival of communications facilities under the most severe natural phenomena. The INMARSAT system has been proven successful in emergency and recovery operations resulting from several hurricane events in recent years.

VA CALIFORNIA EMERGENCY COMMUNICATIONS SYSTEM

The VA's Southern California Emergency Communications System ultra high frequency radio system is being integrated into the Los Angeles Federal Government Wireless Trunking Network. Conversion from the existing analog, shared frequency radio system to the wide-area, digital trunking system will provide service to a widely expanded area with a vastly increased capacity for voice, secure voice, and data communications. The Federal Trunking System is linked to all Federal and civil emergency service and law enforcement providers in the Los Angeles Basin.

CENTRAL INTELLIGENCE AGENCY (CIA)

NS/EP TELECOMMUNICATIONS MISSION

The NS/EP telecommunications mission of the CIA is to ensure the secure flow of all-source foreign intelligence information to the President and other selected national policy makers. To this end, CIA provides secure, rapid, and reliable round-the-clock telecommunications and information services that are:

- Modern, efficient, and interoperable to support intelligence collection and distribution requirements
- High volume and timely for open-source collection
- Quick reacting in support of crises and special operational requirements wherever needed.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Office of Communications and Agency Technology Services, under the Deputy Director of Administration, operates, manages, and maintains the CIA's messaging, telecommunications, and information services capabilities.

The agency also provides telecommunications support to other U.S. Government departments and agencies, and the military services as required to support intelligence requirements.

CURRENT/ONGOING TELECOMMUNICATIONS ACTIVITIES

The following CIA activities support NS/EP objectives:

- Assignment of a full-time CIA detailee to the Office of the Manager, National Communications System
- Active participation in the National Communications System activities of the Committee of Principals/Council of Representatives
- Continued support of the Government Emergency Telecommunication Services (GETS), the Federal Telecommunications Standards Committee, the Telecommunications Service Priority System, and the Shared Resources High Frequency Radio Program.

CIA SIGNIFICANT ACCOMPLISHMENTS

Continued to develop a cadre of personnel prepared to meet operation, technical, and system management requirements of modern telecommunications and automated information systems.
Provided enhanced telecommunications services between the CIA and the U.S. military services.
Continued to expand CIA-wide participation in NS/EP GETS activities.
Continued support to Defense Message System objectives and architecture.

FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)

NS/EP TELECOMMUNICATIONS MISSION

FEMA's mission is to reduce the incidence of loss of life and property and protect U.S. institutions from all hazards by leading and supporting the Nation in a comprehensive, risk-based emergency management program of mitigation, preparedness, response, and recovery.

FEMA'S NS/EP TELECOMMUNICATIONS STRATEGIC PLAN AND GOALS

The Agency's Five-Year Strategic Plan has three major goals:

- Protect lives and prevent the loss of property from all hazards
- Reduce human suffering and enhance the recovery of communities after disaster strikes
- Ensure that FEMA serves the public in a timely and cost-effective manner.

PROGRAM ACTIVITIES

In fiscal year (FY) 1999, FEMA continued to develop and coordinate its all-hazards disaster programs among Federal departments and agencies, State and local governments, and other public and private sector organizations. This effort is sustained by a comprehensive national mitigation, preparedness, response, and recovery, all-hazards emergency management capability. Additionally, FEMA functions under the authorities established by the Stafford Act, National Security Decision Directive-97, and Executive Orders 12472 and 12656.

FEMA continued to administer the *Federal Response Plan* and respond to Presidential declarations. FEMA's Mobile Emergency Response Support Detachments were deployed to more than 21 declared disasters. Additionally, FEMA participated in approximately 60 communications tests and provided telecommunications support to special events, such as the North Atlantic Treaty Organization Summit.

As of March 31, 1999, all FEMA mission-critical systems were Year 2000 (Y2K) compliant, as reported in FEMA's quarterly report to the Office of Management and Budget dated May 13, 1999. On June 22, 1999, in a statement before the Committee on Appropriations and the Senate Special Committee on the Y2K Technology Problems, Jacob J. Lew, Director, Office of Management and Budget said, "Fourteen of the 24 major Federal departments and agencies now report that 100 percent of their mission critical systems are Y2K compliant." FEMA was included in those 14 Federal departments and agencies.

FEMA and its Emergency Services Sector partners assessed Y2K readiness of the emergency services community. The readiness of State governments' emergency management organizations has continued to improve through increased Y2K compliance of mission-critical systems and emphasis on contingency planning.

The Agency replaced high frequency (HF) radio system remote control processors at six FEMA Federal Regional Centers with new Y2K-compliant processors. Additionally, FEMA performed corrective maintenance on HF radio systems in 42 State emergency operating centers to ensure operational readiness.

The National Warning System (NAWAS), a nationwide, dedicated landline system, was critical in saving many lives during devastating tornadoes that hit Oklahoma on May 3 and 4, 1999. NAWAS was in constant use during the event, through midnight of the third day. It continuously passed message traffic on damage, spotter reports, and early warning information from the National Weather Service Doppler radar system. The performance of the NAWAS during the Oklahoma event attested to its operational capability.

The National Emergency Management Information System (NEMIS) is an integrated system providing FEMA, States, and other Federal departments and agencies with automation to perform disaster and nondisaster operations. NEMIS supports all phases of emergency management, from State mitigation planning to situation assessments, providing disaster assistance, command and control, programmatic planning, emergency support, and mitigation operations. NEMIS processes all disaster declarations. In June 1999, NEMIS, Version 2, was successfully fielded. It supports the Individual Assistance Program, Public Assistance Grant Program, Hazard Mitigation Grant Program, and the Flood Mitigation Assistance Program.

Project Impact participation by local governments increased to a total of 120, up from 57 communities at the end of FY 1998. Project Impact operates on a common-sense damage-reduction approach, basing its work on preventive actions at the local level, private sector participation, and long-term investments.

FEMA's Internet homepage continues to be popular. In FY 1999, FEMA's Web site increased to nearly 20,000 pages of information, averaging 100,000 visitors each week. A Y2K section was added, and FEMA for Kids added an online magazine and several new games.

UNITED STATES INFORMATION AGENCY (USIA)

NS/EP TELECOMMUNICATIONS MISSION

USIA's Voice of America (VOA) Broadcast System, a validated National Communications System (NCS) asset, is available to the NCS primarily during international emergencies. The Radio Broadcast System, which provides worldwide coverage, is equipped with high-power broadcast transmitters and a staff to coordinate program schedules, facilities, and circuits. The entire staff is available to operate the network with programming material provided by the NCS or its designated representative.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Agency's telecommunications element assigns members to the NCS Committee of Principals/Council of Representatives (COP/COR). The Director of the USIA assigns the authority to implement NS/EP procedures to the COP.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

All actions required under NS/EP and Telecommunications Service Priority (TSP) procedures are being accomplished in close coordination with day-to-day operating facilities that must be operational in emergency conditions. Interoperability considerations are addressed at the time of validation by the NCS. In accordance with the Foreign Affairs Reform and Restructuring Act of 1998, USIA will be integrated into the U.S. Department of State on October 1, 1999. The functions of the United States Information Agency related to international broadcasting will be transferred to the Broadcasting Board of Governors in accordance with title XIII of the act, including functions associated with the International Broadcasting Bureau, the Voice of America, Radio and TV Marti, Radio Free Europe/Radio Liberty, and Radio Free Asia.

THE JOINT STAFF (JS)

NS/EP TELECOMMUNICATIONS MISSION

The Director for Command, Control, Communications and Computer (C4) Systems (J-6) provides advice and recommendations to the Chairman of the Joint Chiefs of Staff and to the Joint Chiefs of Staff, as directed by the Chairman, on C4 matters. He develops policy and plans, monitors programs for joint C4 systems, and ensures adequate C4 support to Commanders in Chiefs, National Command Authorities, and all joint warfighters for joint and combined military operations. He leads the C4 community, conceptualizes future C4 systems architectures, and provides direction to improve joint C4 systems. He oversees C4 support for the National Military Command System.

TELECOMMUNICATIONS STAFF ORGANIZATION

The C4 Systems Directorate (J-6) consists of the Director, a Vice Director, three Deputy Directors (C4 Current Operations, C4 Integration and Requirements, and C4 Assessments, Information Warfare, Resources, and Advance Technologies), and appropriate subordinate divisions. The Director is also the Chairman of the Military Communications-Electronics Board. Each military department has approximately equal representation by rank, number, and importance of billets throughout the directorate. The Director and Vice Director for C4 Systems are general or flag officers from the military departments.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

(Refer to DOD Section)

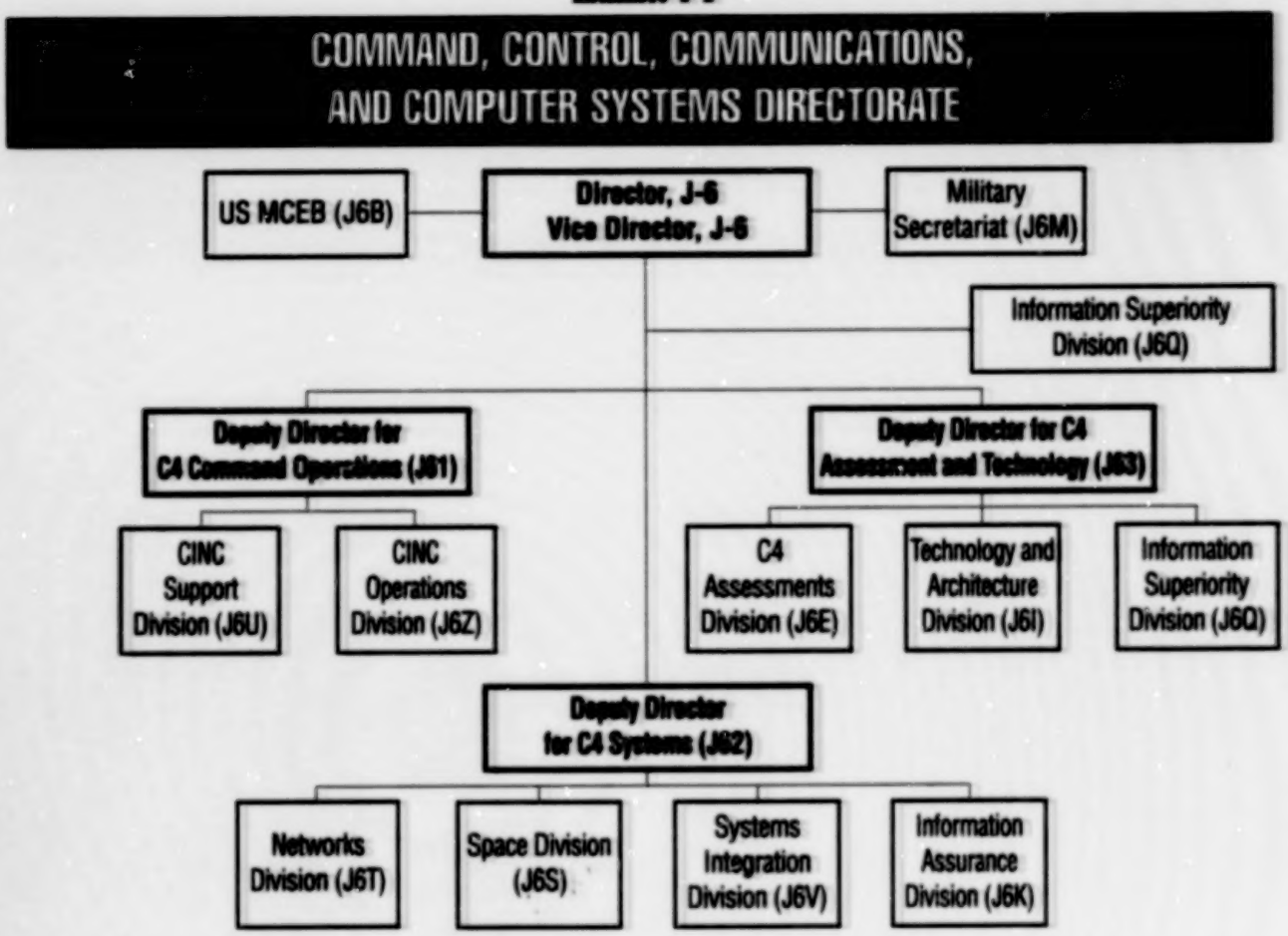
PENDING ISSUES

(Refer to DOD Section)

SIGNIFICANT ACCOMPLISHMENTS

(Refer to DOD Section)

Exhibit 4-1


COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS DIRECTORATE
US MCEB (J6B)
Director, J-6
Vice Director, J-6
Military Secretariat (J6M)
Information Superiority Division (J6Q)
Deputy Director for C4 Command Operations (J61)
Deputy Director for C4 Assessment and Technology (J63)
CINC Support Division (J6U)
CINC Operations Division (J6Z)
C4 Assessments Division (J6E)
Technology and Architecture Division (J6I)
Information Superiority Division (J6Q)
Deputy Director for C4 Systems (J62)
Networks Division (J6T)
Space Division (J6S)
Systems Integration Division (J6V)
Information Assurance Division (J6K)

GENERAL SERVICES ADMINISTRATION (GSA)

NS/EP TELECOMMUNICATIONS MISSION

The General Services Administration (GSA), Federal Technology Service (FTS) NS/EP mission is to provide network services and information technology solutions to ensure federally owned or managed domestic communications facilities and services meet the NS/EP requirements of the Federal civilian departments, agencies, and entities as directed by Executive Order 12474. GSA also provides a Federal Emergency Communications Coordinator to lead Emergency Support Function (ESF) #2 (Communications) as directed by the National Plan for Telecommunications Support in Non-Wartime Emergencies and the Federal Response Plan. This responsibility includes coordinating telecommunications service, provisioning network services and information technology (IT), policy development, and Federal regulatory responsibilities.

CURRENT/ONGOING TELECOMMUNICATIONS ACTIVITIES

- The GSA FTS provides a full range of network services and information technology solutions, and stands ready to meet the current and future needs of the Federal Government with globally positioned resources, services, and solutions. FTS and NS/EP services are also available to tribal governments as well as State and local governments with the sponsorship of a Federal Government department or agency.
- FTS provides contract vehicles for worldwide telecommunications services, international direct distance dialing, wireless voice and data, Internet access, technical services support, and information security services.
- The FTS continues to support the NCS by providing one detailee to the National Coordinating Center (NCC) as Deputy Manager; and 11 Regional Emergency Communications Managers and Federal Emergency Communications Coordinators.
- The FTS provides agencies access to all FTS services, including disaster support, contingency planning, and continuity of operations services through the GSA FTS homepage (http://fts.gsa.gov).
- The FTS has established contract vehicles in response to Presidential Decision Directive 63 (PDD-63) mandates and emergency requirements.
- The FTS Emergency Relocation Center is collocated with the NCS, NCC relocation center, and the Federal Emergency Management Agency (FEMA) Network Operations Center, located at FEMA's Mount Weather facility.

GSA SIGNIFICANT ACCOMPLISHMENTS

The FTS 2001 contract offers competitively priced state-of-the-art comprehensive NS/EP telecommunications services worldwide.

The Metropolitan Area Acquisition contract offers a wide variety of local voice and data services, including the most current, commercially available enhanced NS/EP telecommunication services and technologies with great savings potential.

The GSA Safeguard Contract provides services and products for strengthening the Nation's defense against unconventional threats to the United States, including terrorist attacks, attacks on the critical infrastructure, and cyber attacks.

GSA provided NS/EP telecommunications, housing, security, and resource support to FEMA and other Federal departments and agencies, including State and local governments during Hurricanes Bonnie and Georges; the floods in California, Georgia, Alabama, Louisiana, Mississippi, Kansas, Missouri, and Texas; and the fires in Florida.

GSA FTS is providing leadership across Government in addressing Year 2000 (Y2K) Telecommunications issues through:

- support for the President's Council on Y2K and co-chairmanship with the Federal Communications Commission for the Telecommunications sector Workgroup
- chairmanship for the CIO Council Y2K Telecommunications Subcommittee and facilitating the sharing and exchange of information with Federal agencies
- partnership with industry in collaborative testing of telecommunications equipment
- outreach on Y2K issues to State, local and tribal governments
- ensuring Y2K compliance for all components of the GSA Technology services, including local and long distance contracts.

The GSA FTS Applications 'n Support for Widely-diverse EndUser Requirements (Answer) is a multiple vendor contract vehicle designed to provide a full range of IT support services.

GSA's FTS manages the Federal Computer Incident Response Capability (FedCIRC). In support of PDD-63, "Policy on Critical Infrastructure Protection," FedCIRC provides a central focal point for incident reporting, handling, prevention, and recognition. The purpose is to ensure that the Government has available the critical services needed to withstand or quickly recover from attacks against its information infrastructure.

GSA's FTS manages the Blue Pages Project, a National Performance Review-sponsored Government-wide effort to make the Federal listings in commercial telephone directories easier for the public to understand and to use.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA)

NS/EP TELECOMMUNICATIONS MISSION

The NASA Administrator (pursuant to Executive Order 12656) coordinates with the Secretary of Defense to prepare for use, maintenance, and development of technologically advanced aerospace and aeronautical-related systems, equipment, and methodologies applicable to national security emergencies.

TELECOMMUNICATIONS STAFF ORGANIZATION

NASA's Associate Administrator for the Office of Space Flight has programmatic responsibility for representing the organization, on behalf of the Administrator, in the National Communications System (NCS) process. The Associate Administrator for Space Flight assigned the Director of Space Communications as NASA's Committee of Principals member. The Associate Administrator for Space Flight also assigned NASA's lead center role for Space Operations to the Johnson Space Center, Houston, Texas. The Director, Space Operations Management Office (SOMO) serves as the functional manager for agencywide space operations communications.

NASA's George C. Marshall Space Flight Center, located in Huntsville, Alabama, maintains lead center responsibility for the operation of NASA's telecommunications and data networking infrastructure, known as the NASA Integrated Services Network, one of several operational elements of SOMO.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

NASA continues to support the NCS in achieving its assigned missions and the successful accomplishment of national-level programs approved by the White House. This includes Telecommunications Service Priority, Communications Resources Information Sharing, Federal Telecommunications Standards Program, Cellular Priority Access Service, Enhanced Satellite Capability, Emergency Response Link, and the National Telecommunications Management Structure.

NASA also continues to actively participate in the Shared Resources High Frequency Radio Program, Government Emergency Telecommunications Service, Interagency Committee on Search and Rescue; and the NCS Technology and Standards Accomplishments.

NASA NS/EP TELECOMMUNICATIONS ASSETS

NASA Integrated Services Network supports both spaceflight-critical communication services and day-to-day administrative and scientific applications within the Agency and with international space partners.

NASA Tracking and Data Relay Satellite System is a constellation of geostationary satellites providing almost uninterrupted communications with NASA's Earth-orbiting satellites and other supported customer satellites.

NASA Deep Space Network supports interplanetary satellites, high-Earth orbiting satellites, and radio science missions.

NASA Research & Education Network is NASA's component to the Next Generation Internet initiative. It operates as a testbed for developing Internet technologies, applications, and networking tools.

NASA SIGNIFICANT ACCOMPLISHMENTS

Consolidated four previously autonomous networks and contracts under a single contractor.

Increased capacity and survivability of NASA networking capabilities with Russian space partners to support the communications needs for the International Space Station era.

Established high-performance internetworking capabilities with the Next Generation Internet partners and the university-based Internet2 project under the Presidential Advisory Committee on High Performance Computing and Communications, Information Technology, and the Next Generation Internet.

Awarded contract to consolidate all space operations and communications support activities under a single prime contractor to ensure more effective and efficient operations in all NASA's space research activities.

NUCLEAR REGULATORY COMMISSION (NRC)

NS/EP TELECOMMUNICATIONS MISSION

NRC is responsible for ensuring adequate protection of the public health and safety, the common defense and security, and the environment with respect to the use of nuclear materials for civilian purposes in the United States. Activities licensed and regulated by the Commission include commercial nuclear power reactors; nonpower research, test, and training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste.

The Commission's NS/EP telecommunications provide for reliable connectivity between the NRC Operations Center, operating nuclear power plant control rooms, emergency operations facilities, and regional incident response centers. This connectivity ensures immediate notification to the NRC Operations Center of unusual occurrences and provides relevant information during events at NRC licensed facilities.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

Federal Telecommunications System 2000 (FTS 2000) provides reliable service to all nuclear power plants, associated emergency operations facilities, and major NRC fuel facilities. NRC provides circuits for seven emergency operations functions by multiple lines. The NRC continued to work with the National Communications System (NCS) on an option that would involve using Government Emergency Telecommunications Service (GETS) to provide access to long distance service in lieu of FTS 2000 at nuclear power plants. The NRC has completed its evaluation of options for post-FTS 2000 emergency telecommunications. The current FTS 2000 service will be transitioned to a combination of utility-provided circuits and FTS 2001 service. GETS will figure prominently in this long-term emergency telecommunication solution.

NRC has continued to participate in the Emergency Response Link (ERLink) program, which provides a secure Internet-based platform for exchanging emergency response information. Over the last year, NRC provided information to ERLink in support of three emergency exercises. It is understood that ERLink would soon be hosted on a Federal Emergency Management Agency (FEMA) server. NRC plans to coordinate with NCS and FEMA to ensure that the ERLink functionality that supports NRC response operations continues after its transition to a FEMA server.

The NCS has supported the NRC Year 2000 (Y2K) contingency planning in a number of ways. NCS provided an evaluation of the Y2K status of central offices that serve nuclear power plants in support of NRC's contingency planning effort. NCS also provided comments on the Draft NRC contingency plan and participated in the Y2K TableTop Exercise. The NRC will sponsor all commercial nuclear power plants and major fuel cycle plants for GETS access as part of the Y2K contingency plan effort.

NRC SIGNIFICANT ACCOMPLISHMENTS

NRC used ERLink in three nuclear power plant emergency drills to transfer information, including status summaries and press releases.

NRC encouraged licensee use of GETS as a part of contingency plans.

GETS cards have been ordered for the NRC Resident Inspector offices at all commercial nuclear power plants.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

NS/EP TELECOMMUNICATIONS MISSION

The NTIA NS/EP mission as tasked under Executive Orders 12046, 12472, and 12656 includes serving as the executive branch telecommunications policy adviser to the President, serving as the manager of Federal Government uses of the radio frequency electromagnetic spectrum under all conditions, and serving as a member of the Joint Telecommunications Resources Board. Thus, responsibilities included advising and assisting the President in administering a system of radio spectrum priorities for those spectrum-dependent telecommunications resources of the Federal Government that support national security or emergency preparedness functions.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

In phases, the NTIA/Office of Spectrum Management (OSM) continues to plan and implement a capability for total electronic transfer of Federal spectrum management data and information. It also continues to develop, field, and maintain several spectrum management automation tools for use by Federal spectrum managers to more effectively plan, coordinate, and control use of the radio frequency electromagnetic spectrum during NS/EP and normal conditions. Specific examples of these activities follow:

- Partnered with the Department of Defense's Joint Spectrum Center to develop the SPECTRUM XXI initial operating capability (Version 1), the follow-on spectrum management software to the Joint Spectrum Management System for Windows, for use by all Federal spectrum managers
- Participated in SPECTRUM XXI, Version 1.0 product acceptance, test, and evaluation as well as training validation for this new system that now provides automatic tracking and reporting of frequency assignment proposals, 32-bit processing for all engineering and plotting programs, and other capabilities
- Completed the electronic database relative to all spectrum-dependent systems slated for use in support of a national emergency declared under Section 706 of the Communications Act of 1934, as amended
- Completed review, coordination, and agreement by two subcommittees of the Interdepartment Radio Advisory Committee relative to more than 400 data fields proposed for inclusion in the NTIA/OSM Data Dictionary for use by all Federal spectrum managers
- Completed via a contractor the digitization of documents pertaining to the Interdepartment Radio Advisory Committee and its Subcommittees, loading of the resultant database on a server, the indexing of all documents, and the installation of a search engine for use by all Federal spectrum managers via CD-ROM as well as a secure Web site.
- Completed the migration of the NTIA Frequency Management Record System from the UNISYS mainframe computer to new workstations, thereby enabling more effective and efficient spectrum support for Federal spectrum managers.

In addition, the NTIA/OSM—

- Participated in National Emergency Management Team Communications Functional Group activities and endeavors
- Participated in Government Emergency Telecommunications Service (GETS) User Council activities and endeavors as well as provided GETS user authorizations to new NTIA emergency essential personnel
- Participated in activities and endeavors of various groups of the President's National Security Telecommunications Advisory Committee
- Participated in NCS Committee of Principals and Council of Representatives activities and endeavors
- Participated in NCS Shared Resources High Frequency Coordination Network Interoperability Working Group activities and endeavors
- Participated in the National Science and Technology Council's Critical Infrastructure Protection Research and Development Interagency Working Group activities.

NTIA SIGNIFICANT ACCOMPLISHMENTS

Established as the Lead Agency for the Information and Communications Sector of the Nation's critical infrastructures
Conducted monthly training classes for Federal spectrum managers in use of the Joint Spectrum Management System for Windows
Participated in a Department of Commerce Infrastructure Asset Evaluation Survey as part of a department-level vulnerability assessment in compliance with Presidential Decision Directive 63
Participated in a telecommunications survey of all Federal departments and agencies and reviewed the draft Integrated Contingency Communications Plan.

NATIONAL SECURITY AGENCY (NSA)

NS/EP TELECOMMUNICATIONS MISSIONS

The National Security Agency (NSA) has an operational mission to support the critical intelligence needs of the Department of Defense (DOD) and national security community and to provide the technical support necessary to develop and maintain the security and protection of NS/EP telecommunications.

TECHNOLOGY AND INFORMATION SYSTEMS SECURITY STAFF ORGANIZATIONS

Within NSA, two organizations share responsibility for supporting NS/EP-related activities. The Technology and Systems Organizations plans and operates the telecommunications systems and networks linking Agency elements worldwide and provides Agency connectivity to other Government services.

The Information Systems Security Organization develops information security (INFOSEC) products and provides services to enhance the security of telecommunications systems. Both organizations work in close collaboration with the military services and defense agencies in support of overall DOD initiatives. In accordance with its National Manager responsibilities under National Security Directive 42, INFOSEC products and services are also applicable across the Government for the protection of classified and sensitive national security information. NSA's customers include a broad range of users of the National Information Infrastructure (NII) and critical infrastructure community and involve a close working relationship with the National Institute of Standards and Technology.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

- Supported the ongoing activities of DOD's Defense-wide Information Assurance Program (DIAP) to provide central oversight and coordination of DOD Information Assurance activities. Key elements of the DIAP include people, operations, and technology. Specific new fundamentals in the technology area include the concept of Defense-in-Depth and the notion of Protect, Detect, and Respond. Detect and respond capabilities include use of intrusion detection tools to identify and react to attacks on information infrastructures. Development of the Information Assurance (IA) Technical Framework was a key contribution in providing overall architectural guidance for the DIAP.
- Developed a high-assurance, robust Key Management Infrastructure for the national security community.
- Developed accreditation procedures through the National Information Assurance Partnership to advance processes for approving commercial INFOSEC products and services in accordance with the International Common Criteria for Information Technology Security. Sponsored more than 12 protection profiles for products and systems.
- Provided services, including threat, vulnerability, and risk assessments to member organizations. The outcome of these services is often security guidance and advice, especially with respect to dependence on the NII.
- Assumed, in partnership with the Defense Information Systems Agency, leadership of the DOD Public Key Infrastructure Program Management Office.
- Continued support of the Critical Infrastructure Assurance Program.
- Continued to lead the activities of the National Security Telecommunications Information Systems Security Committee for ASD/C3I.
- Continued to evolve the Information Assurance Solution Strategy to make available a set of products to construct secure computer networks in support of a wide variety of missions. NSA's approach is to work closely with customers and commercial information technology vendors to completely understand their present and future needs. As a result of this approach, the technological underpinning of the strategy is driven by information management approaches and existing constraints rather than by independent security solutions. Solutions and products collectively provide:
  - Writer-to-reader information security services, including data integrity and access control.
  - Support for applications, such as electronic mail and file transfer.
  - Protection against unauthorized disclosure or modification of information while enabling the integration of systems with different sensitivity levels.
- Provided security guidance for ongoing NCS programs, including Government Emergency Telecommunications Service and Emergency Response Link.

UNITED STATES POSTAL SERVICE (USPS)

NS/EP TELECOMMUNICATIONS MISSION

The U.S. Postal Service has not been assigned any specific NS/EP telecommunications responsibilities in the event of a national emergency or other declared disaster. Therefore, the USPS designs telecommunications systems and services to support day-to-day organizational, administrative, and operational mission requirements. Telecommunications facilities dedicated specifically to NS/EP are limited in scope.

USPS SIGNIFICANT ACCOMPLISHMENTS

During fiscal year (FY) 1999, the USPS continued the rollout of the Associate Office Infrastructure (AOI) program in support of the national deployment of Point of Service (POS1) systems. The Distributed Systems/Central Management Facility (DS/CMF) in Raleigh, North Carolina, opened in FY 1998 to provide a full range of support and remote management services for Novell and Windows NT servers. The USPS achieved their goal of implementing this standard service suite at over 8,000 USPS retail locations by the end of FY 1999. Currently, the Postal Service maintains the world's largest Novell Netware Directory Structure (NDS), with over 265,000 network objects in the NDS tree, and more than 1,300 Novell servers providing access to over 110,000 user accounts.

During FY 1999, the Postal Service began deploying Very Small Aperture Terminal (VSAT) satellite transceiver systems. VSAT services were deployed to over 3,500 large associate offices (LAOs) nationwide to provide a back-up communications path for dedicated terrestrial frame relay services. These new systems replaced previously deployed ISDN services. Deployment of more than 8,000 VSAT systems as backup communications paths will continue throughout FY 2000. In addition, VSAT services were deployed as the primary communications path at over 200 sites to support small associate office (SAO) POS1 deployment. The USPS anticipates installation of these VSAT systems and services at up to 25,000 facilities nationwide. While these systems allow network connectivity for data applications, other services including broadcast video, distance learning and digital radio applications are being considered for use over VSAT systems.

The Delivery Confirmation contract was awarded to Lockheed-Martin Federal Systems during FY 1998 with full deployment achieved during FY 1999. This program provides hand-held Mobile Data Collection Devices (MDCDs) which scan and track bar-coded mail products to approximately 250,000 mail carriers nationwide.

In addition to daily computing and network operational responsibilities, the Information Systems organization also certified over 400 new national-level applications and performed interoperability testing of Common Off The Shelf products on standard computing system platforms.

USPS has aggressively addressed Year 2000 (Y2K) compliance on a national scale. During FY 1999, USPS completed Y2K upgrades of all national data applications, including 137 Severe and Mission Critical and over 285 Important, but Not Critical applications. The Postal Service reviewed all Network Infrastructure Components, including data network (i.e., transmission control protocol/Internet protocol) routers, Electronic Digital Private Branch Exchange (EDPBX), and Electronic Key telephone systems, to ensure Y2K compliance. During FY 1999, USPS also procured over 100 new EDPBX systems and over 800 new Electronic Key telephone systems, while completing Y2K compliance upgrades for over 250 EDPBX systems and over 160 Key telephone systems were completed.

During FY 1999, the Postal Service completed the annual update to the USPS Infrastructure Tool Kit and the Postal Computing Environment Handbook. These documents provide a standardized information technology architecture that defines the evolving computing and telecommunications infrastructure. This architecture follows a utility company model to focus on the infrastructure required to deliver a standard suite of services to all users located in field facilities.

75

FEDERAL RESERVE BOARD (FRB)

NS/EP TELECOMMUNICATIONS MISSION

The FRB's NS/EP responsibilities relate to the "maintenance of the economic posture," and in particular, the "maintenance of national monetary, credit, and financial systems." The FRB does not have telecommunications assets listed as National Communications System (NCS) primary assets. Federal Reserve Banks, not the FRB, own or lease the Federal Reserve System's significant telecommunications assets.

TELECOMMUNICATIONS STAFF ORGANIZATION

The Assistant Director of the Information Technology program in the Board's Division of Reserve Bank Operations and Payment Systems has responsibility for oversight of the Federal Reserve Banks' telecommunications services and serves as a liaison member on the NCS Committee of Principals.

CURRENT/ONGOING NS/EP TELECOMMUNICATIONS ACTIVITIES

The FRB supports NCS initiatives designed to provide essential telecommunications services needed to maintain the Nation's financial telecommunications infrastructure and payment systems. In addition, the FRB continues to sponsor Telecommunications Service Priority (TSP) assignments for essential telecommunications services supporting large-value payment systems, Federal Reserve open market and foreign operations, and the automated auction processing system for Treasury securities. The FRB also continues to sponsor the Government Emergency Telecommunications Service (GETS) for essential Federal Reserve Bank services.

FRB SIGNIFICANT ACCOMPLISHMENTS

The FRB focused its NS/EP activities on its sponsorship role for assigning TSP status, primarily at restoration level four, to essential telecommunications services under criteria it adopted in 1993. By the end of fiscal year 1999, the FRB will have sponsored 1,018 active TSP assignments.

The FRB continues to sponsor a TSP assignment for circuits used for Fedwire funds transfer and securities transfer services, including access circuits to the Fedwire network from depository institutions that engage in large-dollar Fedwire transactions.

The FRB is sponsoring a TSP assignment for circuits used by other payment systems (e.g., The Society for Worldwide Interbank Financial Telecommunications) that meet FRB's eligibility criteria.

The FRB is implementing GETS across the Federal Reserve System to support communications within the Federal Reserve System and with depository institutions in the event of a disaster or communications disruption.

FEDERAL COMMUNICATIONS COMMISSION (FCC)

Most of the FCC's rulings and related activities will either directly or indirectly affect the NS/EP telecommunications activities of other Government departments and agencies. The following text relates some of the actions the FCC has taken during the fiscal year.

YEAR 2000

- Released the Year 2000 (Y2K) Communications Sector Report, which summarizes the status of Y2K remediation in the communications industry. The report covers wireline telephone, wireless telephone, cable television, broadcast television and radio, satellite, international telephone networks, and emergency services.
- Conducted special forums with representatives from the communications industry.

PROVIDING COMMUNICATIONS OPPORTUNITIES

- Proposed to allocate spectrum for a wireless medical telemetry service.
- Adopted rules that facilitate "centralized trunking" by private wireless spectrum users. This action will promote spectrum efficiency through consolidation and better coordination of private wireless systems.
- Adopted three mechanisms that will enable more wireless 911 calls to be completed: "Automatic A/B Roaming–Intelligent Retry," "Adequate/Strongest Signal," and "Selective Retry."
- Proposed to license new 1,000-watt and 100-watt low-power FM radio stations. Sought comments on the possibility of establishing a third "microradio" class at power levels ranging from 1 to 10 watts.
- Streamlined the FCC's Equipment Approval Procedures. This will reduce the time it takes to bring new devices to the market, and it will decrease barriers to international trade.
- Adopted an order addressing the way the FCC measures and predicts strength of television signals for purposes of the satellite Home Viewer Act. The rule is designed to better identify which consumers can or cannot receive their local television broadcasts.

TELEPHONE BILLS

- Adopted principles and guidelines that, by compelling carriers to make the language in phone bills clearer, will make it easier for all consumers to understand their bills.

TECHNICAL ADVISORY COUNCIL

- Formed a Technical Advisory Council. Because it comprises a diverse array of recognized technical experts, the council's collective expertise will help the Commission stay abreast of innovations and developments in the communications industry.

MERGERS

- Approved the merger between SBC Communications, Inc. and Southern New England Telecommunications Corporation.

ENFORCEMENT

- Issued citations to alleged violators of the Telephone Consumer Protection Act. The nature of the violation was sending unsolicited advertisements to consumers' telephone facsimile machines.
- Handled more than 1,200 interference complaints from Federal, State, and local public safety emergency officials.
- Completed audits of the-then seven Regional Bell Operating Companies' hard-wired central office equipment and released those reports.
- Issued notices of apparent liability to companies engaged in slamming. Slamming is the practice of changing a consumer's communications service provider without the consumer's express consent. Examples of liability assessments are—

  Business Discount Plan—$2.4 million.
  Long Distance Direct, Inc—$2.0 million.
  Local Long Distance—$1.12 million.
  Vista Group International—$1.0 million.

CALEA TECHNICAL STANDARDS

- Adopted technical requirements for wireline, cellular, and broadband personal communications services (PCS) carriers to comply with the provisions of the Communications Assistance for Law Enforcement Act of 1994 (CALEA). Congress enacted CALEA to ensure that telecommunications carriers' facilities are capable of executing legally authorized electronic surveillance. Specifically, the FCC required that all capabilities of the Telecommunications Industry Association interim standard (J-STD-025) and six of nine "punch list" capabilities requested by the Department of Justice/Federal Bureau of Investigation be implemented by wireline, cellular, and broadband PCS carriers. These capabilities will help ensure that law enforcement can take advantage of the most up-to-date technology to fight crime. In defining the requirements, the Commission weighed law enforcement's needs against the right of all Americans to privacy, and the cost to industry of providing these tools to assist law enforcement.

A

NCS RELATED ACRONYMS

78

NCS RELATED ACRONYMS

A	
ACR	Alternate Carrier Routing
ADM	Office of Administration
ADSL	Asymmetric Digital Subscriber Line
AIN	Advanced Intelligent Network
ALMA	A Logical Modernization Approach
ANSI	American National Standards Institute
Answer	Applications 'n Support for Widely-Diverse EndUser Requirements
ATM	Asynchronous Transfer Mode
B	
BOP	Bureau of Prisons
C	
C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computers
CCPC	Civil Communications Planning Committee
CIA	Central Intelligence Agency
CINC	Commander in Chief
CIP	Critical Infrastructure Protection
CLEC	Competitive Local Exchange Carriers
CMC	Crisis Management Center
COMSEC	Communications Security
COOP	Continuity of Operations Plan
COP	Committee of Principals
COR	Carrier Operated Relay
COR	Council of Representatives
CPAS	Cellular Priority Access Service
CPS	Cellular Priority Service
CRIS	Communications Resource Information Sharing
CSO	Communications Services Office
D	
DEA	Drug Enforcement Administration
DIAP	Defense-wide Information Assurance Program
DISA	Defense Information Systems Agency
DMS	Defense Message System
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy

DOI	Department of the Interior
DOINET	Department of the Interior Network
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DSN	Deep Space Network
DTS	Diplomatic Telecommunications Service
DWDM	Dense Wave Division Multiplexing

E

EC	Electronic Commerce
ECN	Emergency Communications Network
E.O.	Executive Order
EOC	Emergency Operation Centers
EOT	Emergency Operations Team
EOUSA	Executive Office of United States Attorneys
ERLink	Emergency Response Link
ERT	Emergency Response Training
ESC	Enhanced Satellite Capability
ESF#2	Emergency Support Function #2

F

FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FedCIRC	Federal Computer Incident Response Capability
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FLEWUG	Federal Law Enforcement Wireless Users Group
FOC	Full Operational Capability
FOIA	Freedom of Information Act
FRB	Federal Reserve Board
FRP	Federal Response Plan
FTR	Federal Telecommunications Recommendations
FTS	Federal Technology Service
FTSC	Federal Telecommunications Standards Committee
FWUF	Federal Wireless Users Forum
FY	Fiscal Year

G

GETS	Government Emergency Telecommunications Service
GII	Global Information Infrastructure
Global	Global Criminal Justice Information Network
GSA	General Services Administration

H

HAPS	High Altitude Platform Stations
HF	High Frequency
HPC	High Probability of Completion

I

IA	Information Assurance
IAW	Indications, Assessment, and Warning
IC	Integration Contract
ICC	Information Coordination Center
IDCU	Integrated Data Communications Utility
IDSG	Intrusion Detection Subgroup
IES	Industry Executive Subcommittee
IIG	Information Infrastructure Group
IMT-2000	International Mobile Telecommunications-2000
IN	Intelligent Network
INEEL	Idaho National Engineering and Environmental Laboratory
INFOSEC	Information Systems Security Organization
INMARSAT	International Maritime Satellite Organization
INS	Immigration and Naturalization Service
IOC	Initial Operational Capability
IP	Internet Protocol
IRM	Information Resources Management
ISAC	Information Sharing and Analysis Center
ISDN	Integrated Services Digital Network

ISPG	Information Security Policy Group
IT	Information Technology
ITU	International Telecommunication Union
IXC	Interexchange Carrier

J

J-6	Command, Control, Communications, and Computer Systems Directorate
JABS	Joint Automated Booking Station
JAMS	Justice Automated Message System
JCN	Justice Consolidated Network
JCS	Joint Chiefs of Staff
JMD	Justice Management Division
JTRB	Joint Telecommunications Resources Board

L

LC	Limited Capability
LEC	Local Exchange Carrier
LMR	Land Mobile Radio
LNP	Local Number Portability
LRG	Legislative and Regulatory Group
LTA/EPA	Late Trans-Attack and Early Post-Attack

M

MAA	Metropolitan Area Acquisition
MARAD	Maritime Administration

N

NANPA	North American Numbering Plan Administrator
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NAWAS	National Warning System
NCA	National Command Authorities
NCC	National Coordinating Center for Telecommunications
NCS	National Communications System
NDAC	Network Design and Analysis Center
NEMIS	National Emergency Management Information System
NESDIS	National Environmental Satellite Data and Information Service
NG	Network Group
NISN	NASA Integrated Services Network
NII	National Information Infrastructure
NIIF	Network Interconnection and Interoperability Forum
NIST	National Institute of Standards and Technology
NMCS	National Military Command System
NOAA	National Oceanic and Atmospheric Administration
NPA	Numbering Plan Area
NRC	Nuclear Regulatory Commission
NREN	NASA Research & Education Network
NRIC	Network Reliability and Interoperability Council
NSA	National Security Agency
NSC	Norton Systems Center
NSDU	Norton Software Distribution Utility
NSIE	Network Security Information Exchanges
NS/EP	National Security and Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NTCN	National Telecommunications Coordinating Network
NTIA	National Telecommunications and Information Administration
NV	Nevada Operations Office
NWS	National Weather Service

O

OA	Operating Administrations
OC	Oversight Committee
OET	Office of Emergency Transportation
OMNCS	Office of the Manager, National Communications System
OPGW	Optical Group Wire
OPT	Office of Priority Telecommunications

81

OSG	Operations Support Group
OSM	Office of Spectrum Management
OSTP	Office of Science Technology and Policy
OTN	Optical Transport Network

P

PACA-E	Priority Access and Channel Assignment-Enhanced
PBX	Private Branch Exchanges
PCS	Personal Communications Services
PDD-63	Presidential Decision Directive 63
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PL	Planning Letter
PMO	Program Management Office
PN	Public Network
POTS	Plain Old Telephone Service
PPBS	Planning, Programming, and Budgeting System
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
PWDS	PCS and Wireless Data Services

R

R&D	Research and Development
RBOC	Regional Bell Operating Companies
RECP	Regional Emergency Communications Planners
RISC	Regional Interagency Steering Committee
RSPA	Research and Special Programs Administration

S

SARSAT	Search and Rescue Satellite
SHARES	Shared Resources Program
SOMO	Space Operations Management Office
SONET	Synchronous Optical Networks
Southwestern	Southwestern Power Administration
SR	Savannah River Operations Office
SS7	Signaling System 7

T

TCC	Transportable Communications Centers
TCP/IP	Transmission Control Protocol/Internet Protocol
TDRSS	Tracking and Data Relay Satellite System
TERS	Training, Exercise, and Regional Support
TESP	Telecommunications Electric Service Priority
TREAS	Department of the Treasury
TSP	Telecommunications Service Priority Program
TSS	Telecommunications Services Staff

U

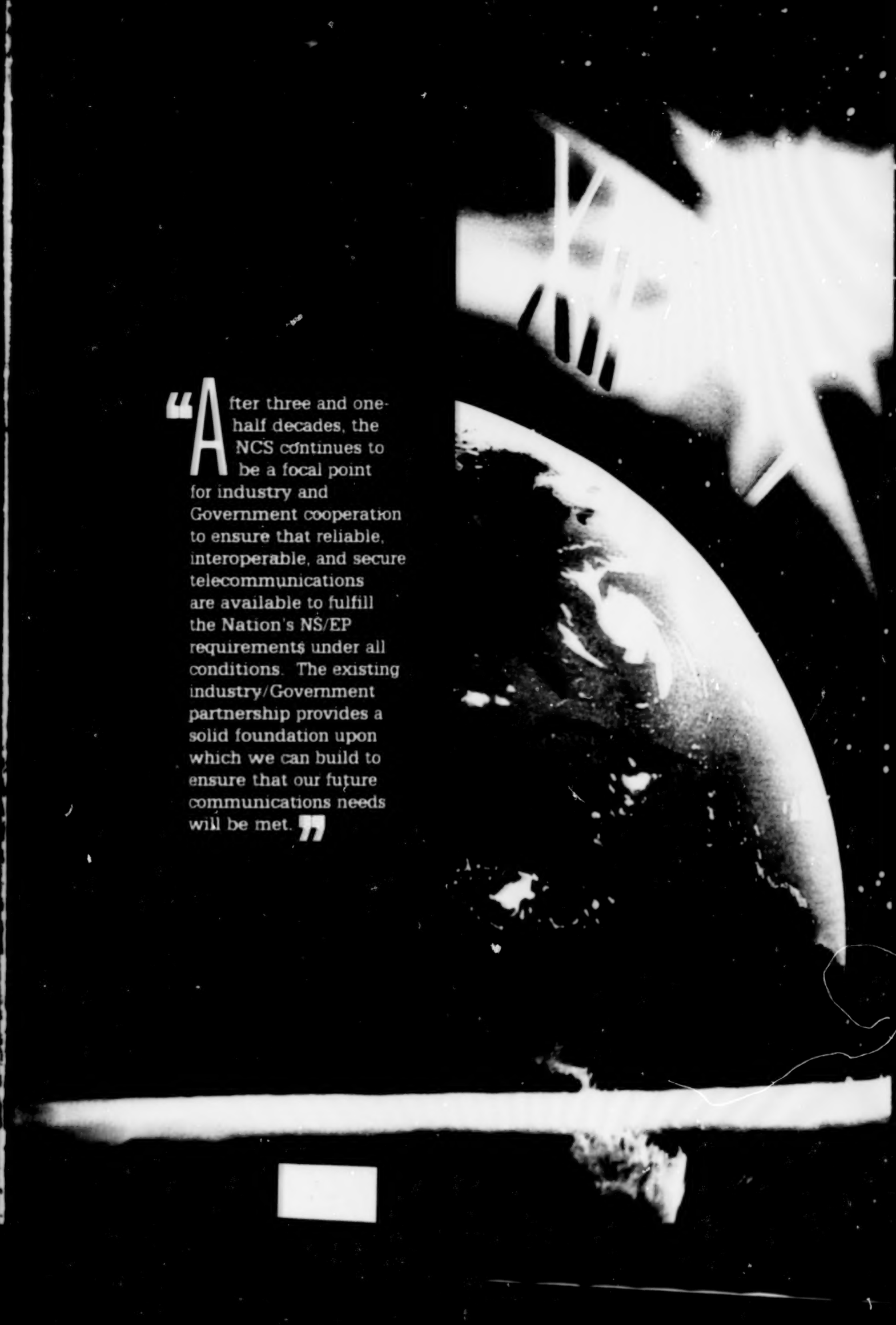
UAV	Unmanned Aerial Vehicles
U.K.	United Kingdom
U.S.	United States
USCG	United States Coast Guard
USDA	United States Department of Agriculture
USIA	United States Information Agency
USMS	United States Marshals Service

V

VA	Department of Veterans Affairs
VANTS	Department of Veterans Affairs Nationwide Teleconferencing System
VHF	Very High Frequency
VISN	Veteran's Integrated Service Network
VMR	Voice Modulation Recognition
VOA	Voice of America

Y

Y2K	Year 2000



"After three and one-half decades, the NCS continues to be a focal point for industry and Government cooperation to ensure that reliable, interoperable, and secure telecommunications are available to fulfill the Nation's NS/EP requirements under all conditions. The existing industry/Government partnership provides a solid foundation upon which we can build to ensure that our future communications needs will be met."

END

07-25-00